航 空 航 天

CHINA AEROSPACE
STUDIES INSTITUTE

In Their Own Words:
Foreign Military Thought

Lectures on Joint Campaign Information Operations

Printed in the United States of America
by the China Aerospace Studies Institute

ISBN 9798486866630

To request additional copies, please direct inquiries to
Director, China Aerospace Studies Institute,
Air University, 55 Lemay Plaza, Montgomery, AL 36112

E-mail: Director@CASI-Research.ORG
Web: http://www.airuniversity.af.mil/CASI
https://twitter.com/CASI_Research @CASI_Research
https://www.facebook.com/CASI.Research.Org
https://www.linkedin.com/company/11049011

China Aerospace Studies Institute

CASI's mission is to advance understanding of the capabilities, development, operating concepts, strategy, doctrine, personnel, organization, and limitations of China's aerospace forces, which include: the PLA Air Force (PLAAF); PLA Naval Aviation (PLAN Aviation); PLA Rocket Force (PLARF); PLA Army (PLAA) Aviation; the PLA Strategic Support Force (PLASSF), and the civilian and commercial infrastructure that supports the above.

CASI supports the Secretary, Chief of Staff of the Air Force, the Chief of Space Operations, and other senior Air and Space leaders. CASI provides expert research and analysis supporting decision and policy makers in the Department of Defense and across the U.S. government. CASI can support the full range of units and organizations across the USAF, USSF, and the DoD. CASI accomplishes its mission through conducting the following activities:

- CASI primarily conducts open-source native-language research supporting its five main topic areas.
- CASI conducts conferences, workshops, roundtables, subject matter expert panels, and senior leader discussions to further its mission. CASI personnel attend such events, government, academic, and public, in support of its research and outreach efforts.
- CASI publishes research findings and papers, journal articles, monographs, and edited volumes for both public and government-only distribution as appropriate.
- CASI establishes and maintains institutional relationships with organizations and institutions in the PLA, the PRC writ large, and with partners and allies involved in the region.
- CASI maintains the ability to support senior leaders and policy decision makers across the full spectrum of topics and projects at all levels, related to Chinese aerospace.

CASI supports the U.S. Defense Department and the China research community writ-large by providing high quality, unclassified research on Chinese aerospace developments in the context of U.S. strategic imperatives in the Asia-Pacific region. Primarily focused on China’s Military Air, Space, and Missile Forces, CASI capitalizes on publicly available native language resources to gain insights as to how the Chinese speak to and among one another on these topics.

PROJECT EVEREST

The Department of Defense epicenter for human-centered strategic art

Project Everest is a strategy design start-up inspired by Andrew Marshall's call to cultivate comprehensive understanding of U.S. competitors in pursuit of national security. Project Everest contributes to this vision in two fundamental ways: by recurrently educating defense professionals on adversaries' ways of war and by facilitating the development of novel strategies that achieve competitive advantage over potential adversaries. Founded in 2013, Project Everest has grown its membership to hundreds, and shaped policy and education campaigns at the national level.

Project Everest tackles two significant national security problems for our nation. First, Project Everest seeks to invigorate the Chairman of the Joint Chiefs' 2013 charge to develop an officer cadre with deep regional expertise and to answer the 2018 National Defense Strategy's charge to "prioritize developing the intellectual firepower of our warfighters and workforce via education and training".

Second, we seek to inject creativity into stale strategy development methods for the Department of Defense, inspiring novel approaches to competition and warfighting and answering the charge of the 2021 Interim National Security Strategic Guidance to employ our "full diversity of talents [to] address today's complex challenges" and "prevail in strategic competition." Traditional approaches to strategy development overlook opportunities to understand how a potential adversary thinks about and plans for competition and war.

We bring together motivated individuals with subject-matter expertise in their primary specialty to interrogate key strategic issues throughout their careers. Over time, this develops a cadre of high-caliber officers who have a deepened appreciation of near-peers' ways of war and are experienced in thinking through the toughest operational and strategic challenges. We believe human-centered design and unconventional problem-solving methodologies enable members to assimilate new knowledge and develop novel warfighting concepts and recommendations to address strategic challenges.

Project Everest was founded by six graduates of the School of Advanced Air and Space Studies, who range in gender, expertise, rank, status, ethnicity, and personality, and who have a shared vision to inspire change in the way our nation prepares to compete and fight.

In Their Own Words

The "In Their Own Words" series is dedicated to translations of Chinese documents in order to help non-Mandarin speaking audiences access and understand Chinese thinking. CASI would like to thank all of those involved in this effort.

In the "In Their Own Words" series, CASI and its collaborators aim to provide Chinese texts that illustrate thoughtful, clearly articulated, authoritative foreign perspectives on approaches to warfare at the strategic, operational, and tactical levels.

Project Everest Comments

Lectures on Joint Campaign Information Operations is part of the Project Everest "Foreign Military Thought" series. This particular volume was published under the auspices of Project Everest in conjunction with the China Aerospace Studies Institute. Written by the PRC's National Defense University (NDU) faculty, with assistance from the General Staff Operations Department and the Academy of Military Sciences, this text contains instructional material for NDU Commander's Course, Staff Officer, and PLA-wide Information Operations Advanced Studies Courses. Forward looking, and deliberately very comprehensive on concepts of information operations at the campaign level in the joint form, the 2009 edition contains extensive review/revisions from its previous publications.

The U.S. editors apply a stringent vetting process to select foreign texts. Selected texts will help build a deep understanding of different approaches to warfare and clarify details of foreign perspectives that may have both commonalities and asymmetries to U.S. approaches. This series will stimulate thought on both the core elements of military strategy and operational concepts for force application during war. CASI and Project Everest believe that cultivating a holistic understanding of foreign perspectives by learning from high-quality original material articulated from a foreign perspective offers an invaluable starting point for the exchange of ideas and the development of military thought.

Translators' Notes

This translation of the original text aims to accurately capture the technical meanings, in both English and Chinese. This will ensure that the reader will not inadvertently draw the wrong substantive understanding based on inaccurate translations.

Note on Trouble Terms:

Throughout the text are certain terms that are translated with the Chinese pinyin modifying the terms. This convention allows the reader to distinguish nuances that exist in the Chinese terms.

Jihua and *guihua* plans. The *jihua* plan is a more specific plan, a plan that is meant to be carried out to the letter, whereas the *guihua* plan is a more general plan that is macroscopically focused. In order to retain the intended Chinese distinction, the *jihua* plan is rendered as "plan {*jihua*}" due to its prevalence in this translation. The *guihua* will be rendered in a more customary fashion of *guihua* plan.

Bushi and *bushu* dispositions. *Bushi* disposition is the *mission differentiation*, *organized grouping,* and *positioning* [deployment] accomplished for strengths within the campaign task-based organization. *Bushi* denotes the relationship between one's own military forces, the opponent's military forces, and the combat environment (e.g., terrain). *Bushu* disposition is the positioning of participating force-strengths for a fixed time and space on the basis of *mission differentiation* and the *organized grouping of campaign* and in accordance with operational conditions and the enemy's possible activities.

Xitong, tixi, tizhi, and *zhidu* systems. The system {*xitong*} is an elemental system, one that can operate on its own. The *tixi*-system is similar conceptually to a *System of Systems* as often seen in systems engineering; in Chinese, a *tixi*-system is understood to be composed of elemental systems {*xitong*} acting together as a larger whole. The *tizhi*-system is a large-scale system, typically a national-scale system and understood to be formalized embodiment of a *zhidu*-system. The *zhidu*-system describes a conformance system, one where all elements of that system conform to how that system is defined.

Note on Table of Contents:

The double pagination shown in the Table of Contents represents: 1) the original page numbers from *Lectures on Joint Campaign Information Operations* followed by 2) the actual page number of this translation. Additionally, the headings throughout the document also reference original page numbers from the original-language text.

Lectures on Joint Campaign Information Operations

联合战役信息作战教程

{*lianhe zhanyi xinxi zuozhan jiaocheng*}

Yuan Wenxian {袁文先}, Chief Editor

National Defense University Press

CIP

(Beijing) New Registration No. 120

Lectures on Joint Campaign Information Operations
Yuan Wenxian {袁文先}　　Chief Editor

Published and Distributed by: National Defense University Press
Address: A3 Hongshankou, Haidian District, Beijing City
Zip Code: 100091
Telephone: (010) 66769235
Responsible Editor: Wang Li dong {王立东}

Printed by: Beijing Ziruili Printing LLC
Book Size: 880 x 1230 mm　A5
Print Sheet: 14.75
Word Count: 291,000
Edition: November 2009, 1st Edition, 1st Print
Unified Book Number: 5 5626-570

Editors and Authors

Chief Editor: Yuan Wenxian {袁文先}

Associate Editors: Guo Ruobing {郭若冰} Zhang Jian {张健}

Writers: Yuan Wenxian {袁文先} Guo Ruobing {郭若冰} Zhang Jian {张健}
Zhang Pengfei {张鹏飞} Chen Fengbin {陈凤滨} Wei Konghu {魏孔虎}
Yang Qiaoling {杨巧玲} Huang Yuliang {黄玉亮} Xu Xiaogang {徐小刚}
Chen Xiaolong {陈肖龙} Qi Shengli {齐胜利} Huang Xianjun {黄贤军}
Wang Runbu {王润补} Yuan Yudao {袁玉道} Han Chunjiu {韩春久}
Zhang Yang {张阳} Zhu Qigang {朱寄刚} Zhang Jian {张鉴}

Manuscript Compilation: Yuan Wenxian {袁文先} Zhang Jian {张健}
Guo Ruobing {郭若冰} Wang Runbu {王润补} Huang Xianjun {黄贤军}

Preface

Joint campaign information operations [IO] are the series of operational activities adopted for seizing and maintaining local information dominance of a joint campaign, and it is an important operational activity of the joint campaign. It is normally implemented together with other operational activities, and it can even be sometimes independently implemented. The manifested forms of joint campaign information operations mainly are: electronic warfare, network warfare, intelligence warfare, psychological warfare, physical destruct warfare. Amongst these, electronic warfare and network warfare are the main forms of IO. Joint campaign IO is an important component of a joint campaign and it has a major effect on victory or defeat of a campaign. Therefore, strengthening the study of joint campaign IO from theoretical and practical perspectives has a very important significance for improving PLA joint campaign IO capability and gaining victory in a war under informationized conditions.

This lecture is guided by Mao Zedong's military thought, Deng Xiaoping's armed forces building thought in the new era, Jiang Zemin's defense and armed forces building thought, and Hu Jintao's important discourse on defense and armed forces building under new circumstances and it thoroughly implements the scientific development view; with the military strategic concept of the new era as its unified grasp and with the *Chinese PLA Joint Campaign Outline* {中国人民解放军联合战役纲要 *zhongguo renmin jiefangjun lianhe zhanyi gangyao*} as its basis, it focuses on the characteristics and laws of local war under informationized conditions; tightly combines PLA realities; it borrows from the effective methods of foreign IO in recent period local wars; it emphasizes the study of joint campaign IO for the next 5-10 years in the following issues: characteristics, guidance thought and operational principles, operational strengths, operational objectives, basic fighting methods, operational preparations, operational implementation, command modes and adjusting-coordination and control; operational support; **[end of page 1]** logistic support; equipment support; political work; a variety of operational patterns of IO; operational effectiveness evaluations; training; and building {*jianshe*}. It strives to establish a more robust joint campaign IO theoretical *tixi* system, and it provides a theoretical basis for organizing and implementing IO and training by the joint campaign commander and his command organ.

During the course of writing this lecture, we received a high level of attention and enthusiastic support from the concerned experts and leadership of the General Staff Operations Department {*zuozhan bu*}, Electronic Confrontation Department {*dianzi duikang bu*}, Academy of Military Science and National Defense University. We consulted a large number of relevant writings and recent new research achievements in the joint campaign IO domain. Serving as teaching material of used on a trial basis in classes such as the National Defense University's Commanders Course, Staff Officer and PLA-Wide Information Operations Advance Studies Courses, etc. we assimilated ideas and recommendations from scholars and concerned experts; for this we wish to express our heartfelt appreciation.

Due to the limitations of the writing and composition member's research levels, it was difficult to avoid inappropriate parts in this set of teaching materials. We sincerely request our readership to make critiques and corrections.

Authors

November, 2009 **[end of page 2]**

Table of Contents

Chapter 1
Overview of Joint Campaign Information Operations…1

Following the swift development in information technology, information and combat weaponry combined with the platform to produce information weaponry that can greatly increase the combat effectiveness of the weapon system and platform. Information has a very significant place and effectiveness in wars and no war can separate from information. The regional wars since the 80s in the 20th century indicated to the world that information operations had become a new commanding ground to win victory in modern war, its place in modern war was increasing and the constant in-depth theories on information operations following the implementation of wars had emerged at the right moment.

Section 1: Relevant Concepts in Joint Campaign Information Operations…1

Joint campaigns actually started entering into the war in Second World War. At that time, the major operational activities on the battlefield were accomplished by a campaign force of military services such as the Army, Navy, and Air Force. Following the constant development in information technology, operation space had also expanded and the original traditional operation spaces on land, sea and air had been extended to the information space. In 1991, with the Gulf War as the symbol, information had become the most important operation source in joint campaigns. Through information attacking and defending operations, one can be in control of the joint campaign situation and the joint campaign had emerged with a new operational activity that was the information operation. The implementation of regional wars under the condition of information indicated that the emergence of information operations had expedited the development in establishing the theory on information power and information operations with the goal of seizing the information power control had become an important component of the joint campaign, so the seizing of control in information power meant the seizing of initiative in joint campaigns.

In January 1999, the Chinese military officially issued the *Guidelines for Chinese People's Liberation Army Joint Campaign* and it was the first time the "information operation" was officially listed in the operational ordinance, signifying that Chinese military joint campaign information operations theoretical research had entered into a new development stage.

I. Information operations…2

Information operations are a series of operational activities[1] for seizing and maintaining control of information power. That is a series of operational activities the opposing parties in the battlefield use through measures such as electronic warfare and computer network warfare to take advantage and damage the enemy's information and information system and at the same time, protect one's own information and information system in order to gain free power and initiative in battlefield information. The measure and capability components of the information operations are the keys to understanding the concept of information operations and each nation's military has its own view and understanding. The American military considers "information operations as operational activities that comprehensively utilize core abilities such as electronic warfare, computer network warfare, psychological warfare, military deception, and operations security for the purpose of influencing, damaging, interrupting and depriving the enemy's man-made and automatic decision-making capabilities, at the same time, protecting its own decision-making capability under the coordination of specific support and relevant ability."[2] For the first time, in the 2006 edition's *Regulations of American Military Joint Information Operations*, the American military proposed that information operations included three major capabilities and they were core capability, support capability, and relevant capability. Among them, the information operations core capability included electronic warfare, psychological warfare, computer network warfare, military deception, and operation security; information operations support capability included information safeguard, entity security, entity attack, counter intelligence, and combat photography; information operations relevant capability included public affairs, military-civilian relation activity, and national defense support in public diplomacy.

To have an understanding of information operations, one must mainly have a handle of the following points: (1) from the purpose of operations, seizing the control of information power is the direct purpose of information operations. In the modern military, each combat unit and each weapon system are coagulated to become one operational body through the bonding action of the military information system and if it loses this bonding action, then the military becomes a plate of loose sand. When the opposition's information system is damaged, its operation initiative power is taken away; while one's own information system is protected, its combat force is increased several fold. Therefore, information operations are combats developed surrounding the destruction and protection of the information system and the pursued goal of information operations is to seize information superiority. (2) From the angle of the battlefield environment, the battlefield mentioned here can either be a battlefield of an information

---

[1] *An Introduction to Information Operations* {信息作战概论 *xinxi zuozhan gailun*}: Dai Qingmin {戴清民}, People's Liberation Army Press, published in 2001, p. 25.

[2] Regulations of American Military Joint Information Operations, 13 February 2006.

war pattern, or a battlefield of an information war pattern transitioned from a mechanized war pattern, or even a battlefield of a mechanized war pattern. (3) From the angle of combat object, the enemy's information system is the attack target in information operations. As an attack method, an information operation is not to destroy the enemy's effective strength; neither is it mainly to damage the enemy's military installation but to damage the military information system including the enemy's information detection, information transfer, information processing, and information control that these effective strengths and military installations depend on to become effective. (4) From the angle of operation category, the basic categories of the information operations are information operation reconnaissance, information attack, and information defense. Information operation reconnaissance is mainly to reconnoiter the category, deployment, tactical and technical performance, and operational application method of the enemy's information system in order to provide intelligence support for information attack and defense; at the same time, it also provides intelligence support to other actions in the joint campaign. Information attack mainly interrupts the normal operation of the enemy's information system through all types of attacking methods. Information defense mainly secures the normal effectiveness of one's own information system through information security and information system protection. (5) From the angle of operational type, electronic warfare and computer network warfare are the two major types of information operations. Electronic warfare mainly interrupts the information collection and transmission of the opposition's information system, while computer network warfare mainly destroys the information processing and utilization of the opposition's information system. Through the comprehensive implementation of electronic warfare and computer network warfare that is "computerized electronic integrated warfare {网电一体战 *wangdian yiti zhan*}," one can carry out an overall damage or break down of the enemy's information system. (6) From the angle of operational method, the basic methods of information operations are electronic jamming, electronic deception, virus invasion, computer hacker attack, and anti-radiation destruction and new mechanization information weapon attacks. Virus invasion and computer hacker attack use computer networks to damage the enemy's information processing and utilization. Anti-radiation destruction and new mechanization information weapon attacks destroy the enemy's information platforms and facilities using destructive weapons controlled by information. (7) From the angle of operational activities, operations under information conditions are integrated joint operations of various military services and are mainly indicated in an integrated campaign style of combining various operational types and operational activities, which alter the planar and linear patterns on the battlefield in the past and replace them with a multi-dimensional battlefield pattern that integrates land, sea, air, space, and electromagnetic, thus, creating an integrated command information system, information weapon system using mainly precision guided weapons, and electronic countermeasure system to appear and opening up a new operational domain. In this domain, it finally develops into an information operational activity that is surrounding the seizing of the control of information power due to mutual struggle between information attack and information safeguard. As an important component in a joint campaign, the information operation is a series of operational activities developed to seize and maintain control of information power during the campaign, acts as a lead from the beginning to the end, and is the key to victory in joint operations. (8) From the position and effectiveness of information

operations, the information operation must have organic integration with other operational activities to be effective. The information operation has a profound position and effectiveness in the joint campaign; however, its effectiveness is not all-powerful and it has to have organic integration with other operational activities to fully make use of its power in war. From the angle of war patterns, current war patterns remain "mechanization + information," as information operations do not reject mechanization operations, but use mechanization operations as the basis to increase mechanization operational capability. From the angle of operational effectiveness, even though the position and effectiveness of information operations in the war are getting more profound, the purpose of information operations is mainly to damage the enemy's information system and weapon control system and not to cause direct casualty and destruction of the enemy's military force and combat platforms. From the angle of operational capability, future operations will be an overall combat capability confrontation composed of the mechanical force, defense force, precision attacking capability, and information operation capability and the confrontation process is also the process of mutual action among fire power, mechanical, protection, and information struggle. Information operations must combine with lethality, maneuverability, and protection capability to really show their important value.

In conclusion, as an operation method, the information operation has a specific operational goal and operational target and a special operational type and operational method, so one cannot consider information operations to be able to take on everything in operations and one cannot also ignore the existence of information operations; instead, one must organically combine information operations with other operational methods to form an overall operational capability.

II. Informationized operations…5

As the basic representation form of informationized war, informationized operations {信息化作战 *xinxi hua zuozhan*} deeply reflect the essential characteristics and working patterns of the informationized war.

Informationized operations utilize a large amount of information science and technology to form a command and control system and are integrated operations with other informationized weapons and equipment as the basis; the military is equipped with informationized operation capability within multi-dimensional space such as land, sea, air, space, and electronic; and with joint operations and information operations as major operational forms. Informationized operations is a term with special Chinese military characteristic as the foreign military does not have this term and the concept is comparatively closer to the concept of "network centric warfare" and "rapid decisive operations" proposed by the American military.

To specially indicate the battlefield confrontation format of the informationized war and to understand the essential connotation of informationized operations, one must emphasize the handling of five aspects. (1) Epochal character. Informationized operations

are a product of the information age, high level stage of mechanization operation, and also operational methods that are strictly different from mechanization operations. (2) Regularity. At least one side of the engaging parties should have informationized operational capability that is also the main body of the troop combat capability. The so-called informationized operational capability is the operational capability in which the troops use informationized equipment to carry out early warning detection, command and control, precision attack, and information countermeasures. It is a comprehensive operational capability that combines informational capability with lethality, maneuverability, protection capability, and support capability. (3) Ideological content. In the operational ideology, the prominence of mechanization operations is "platform centric warfare" that uses a large number of mechanized weapon platforms as the basis in battlefield engagement and that is also the major force for gaining victory in the battlefield. The prominence of informationized operations is "network centric warfare" that uses an integrated battlefield informationized network facility of land, air, and space as the basic operational platform and also uses it to communicate and form an integrated overall attacking force to win the victory in the battlefield. (4) Nature of time and space. The major weapon and equipment of informationized operations is the integrated weapon and equipment of land (sea), air, and space and its operational space includes the wide visible battlefield spaces such as ground, sea (under water), air, and space and also includes the invisible spaces such as information, electromagnetic, and psychology. The proportion of the operations being carried out in information space, cognitive space, and psychological space is especially high. (5) Leading nature. The leading function of informationized operations is information and its focalized expression is fire power and substance and the energy of maneuverability. Information not only is a type of operational resource, but also a type of operational energy; at the same time, it is also an adhesive and multiplier of all sorts of operational force and the dominant power to victory in operations.

As a basic operation form in informationized war, the informationized operation has the following differences compared with the basic operation form of the mechanized operation in mechanization war.

On operational purpose, the informationized operation has changed the mechanized operation's method of seizing battlefield initiative by separately seizing air domination, sea supremacy, and land domination on the battlefield in order to have a handle of the military force and fire power superiority in each battlefield space; instead, it uniformly seizes the control of information power, uses information power to influence and restrain the initiative of other battlefields, and thus masters information superiority in the battlefield that is to have a handle on the battlefield real time sense control power, effective operational power of military force and fire power, and smooth operational power of the battlefield service network as the major operational purposes.

On operational target, informationized operation has changed the mechanized operation's operational target of using mainly major engagement of forces and fire power fight to destroy the enemy's effective strength and groups of large number of forces in

order to seize the battlefield space occupation power and strength superiority; instead, its major operational target is to damage and break down the enemy's battlefield "three major systems" – cognitive system, information system, and command and control system; it concentrates on damaging the enemy's informationized battlefield supporting facility and operational basis and weakening and breaking down the enemy's overall operational capability, and thus seizing the battlefield initiative.

On operational form, the informationized operation has changed the mechanized operation's unit-type battlefield contest methods of land, sea, air unit battlefield, unit military service, and unit operational domain; instead, it depends on the informationized battlefield and uses the overall contest among the operational systems consisting of the five major sub-systems – battlefield cognitive system, information system, command and control system, attacking system (including military strength and fire power), and support and safeguard system.

On operational method, the informationized operation has changed the mechanized operation's operational method with direct contact on a vast battle front and carrying out positional attack and defense struggle with assigned campaigns and battles; instead, it uses the "three bodies in one" non-contact operation method consisting of land, air, and space integrated information attack, long-distance precision guided attack on vital points, and large scale strategic air raids.

On the mechanism of getting the upper hand, the informationized operation has changed the mechanized operation's mechanism of getting an upper hand in using superior numbers of military strength and overwhelming strength in fire power; instead, it uses information superiority and superior control of information power to get an upper hand in the battlefield. A superior information system has become the "binder" in binding each operational system, each operation force and various types of weapons and equipment in the battlefield and also is the "multiplier" in leading and manipulating operational forces in the battlefield; therefore, whoever gains information superiority in the battlefield would also gain the initiatives in the battlefield such as air dominance, sea dominance, and electromagnetic dominance.

As a new operational form, the basic development tendency of the informationized operation is mainly indicated as follows.

The battlefield strike has become quick. As precision-guided munitions and others become the major strike measures in the battlefield, the striking speed of the informationized operation has greatly increased. Take the American military as an example; currently, the required time to complete its "strike chain" from discovery, position, aim, attack, to evaluation of the result took 100 minutes in the Gulf War, 40 minutes in the Kosovo War, 20 minutes in the Afghan War, and merely 10 minutes in the Iraq War.

Operational activities have become precise. As highly efficient command information systems and precision-guided munitions become major guided equipment in the battlefield, the development tendency of the informationized operation has become precise. Prior to the Afghan War, the American military had a dispute between two operational theories and the first one was a new war concept of "precision blitzkrieg" proposed by a group led by Secretary of Defense Rumsfeld and it was called "Rumsfeld theory." The second one was the theory of "grand troop operation" proposed by a group led by Secretary of State Powell and it was called "Powell" theory and its main operational idea was to deploy a large number of ground troops, using army heavy divisions to carry out fighting action. The actual war proved that the "precision war" theory in using small size, quickness, and precision to win victory of Rumsfeld was suitable for the actual battlefield; at the same time, it also explains that precision action was the development trend of informationized operations.

Operational procedure has become non-linear. Non-linear operations are an important trend of informationized operations that is to adopt various flexible operational methods based on location, enemy, and situation. Its intention is to attack operations and no longer to gradually "gnaw." Instead, it is possible to directly fight in depth against the enemy's strategy or campaign. Defensive operation is also no longer point-by-point resistant "sustain." Instead, it is possible to deploy strike action against the enemy with the principal force. Counter procedures in operational activities and the phenomenon of irregular "playing card" will occur often.

The battlefield environment has become transparent. The informationized battlefield is no longer operational space composed of natural topography and simple ground fortifications; instead, it is an operational force and activity space that uses man-constructed informationized network facilities as the basis, systems such as land, air and space integrated reconnaissance, communication, command, control, and intelligence as the core, and the striking power of integrated land, sea, air, space, and electronic dimensions as the main body. The "situation on the other side of the mountain" is no longer a blurry picture in the informationized battlefield, but rather has a high level transparency. This high level transparency has changed many uncertainties on the battlefield in the past and has made the targets much more clear and action much more forceful in informationized operations.

III. Joint campaign information operation…9

Regarding the concept of joint campaign information operation, the understanding in the academic world is still not unanimous. Some considered: "Joint campaign information operation is a series of operational activities in a joint campaign utilizing various types of information operational forces and also closely coordinating with other forces in order to seize and maintain information superiority or control of information

power in the battlefield."[3] Based on the above mentioned definition, *Guidelines for Chinese People's Liberation Army Joint Campaign Information Operation* further emphasized the distinct characteristic of information domain confrontation and defined "joint campaign information operation" as "a series of operational activities to be carried out in order to seize and maintain joint campaign regional control of information power and mainly in campaign information confrontation." Information operations create a major influence on the process and result of a joint campaign. On one hand, information operations makes one's own operation to be fully effective through seizing and maintaining information superiority to speed up the joint campaign process and seize campaign victory by laying a firm foundation. On the other hand, information operations cause the enemy to lose battlefield initiative and speed up the enemy's failure through seizing and maintaining information superiority. The effectiveness of the troop combat force as well as effective implementation of operation command and control will mainly depend on the collection, transmission, handling, control, and utilization of operation information. Joint campaign operational activities will be carried out surrounding the seizing of information superiority, the struggle to seize control of information power on the battlefield will raise to a profound position; as a major operational activity in joint campaign, information operations will be on the stage in regional war under informationized conditions and be effective in a leading position.

The essential characteristics of joint campaign information operations are (1) the nature of large space and all time-domain in operation scope. Development in military technology has made the operational space expand constantly. Looking from the flat surface, long distance operation capability of military strength and weaponry has increased unprecedentedly, operational reconnaissance can be carried out in the whole globe and the entire depth of the battlefield, land (sea) weapon range and airplane operational radius have reached thousands of meters, and daily advance speed of military strength maneuvering has reached several hundred thousand meters to greatly expand the operational depth. Looking from the three-dimensional angle, high-tech weapons and equipment will spread out under water, on ground (sea) surface, in air, and even in space, below water as deep as several hundred meters and millions of meters above in space that constitutes a grand three-dimensional operation space and an integrated war in grand crisscross over air, land, and sea and becomes an important characteristic of regional war under informationized conditions. Another characteristic of informationized weaponry is a high level electronics and networking. At the same time information technology has greatly increased the precision, power, and reaction capability of weapons and equipment, it also makes them face the situation of electronic suppression, network attack, and destruction from anti-radiation and new mechanization weapons. Joint campaign information operations certainly follow the informationization of weapons and

[3] *Joint Campaign Information Operations*, National Defense University, Training Department, June 2003.

equipment to penetrate into each domain of the battlefield, its operational space is very broad, and it has clear characteristics of all time domains. (2) The nature of all-depth in striking targets. The several recent regional wars in the world have tentatively shown the inkling of information operations. During the American-Libyan conflict, the American military carried out an overall jamming suppression on the Libyan major electronic facility in the scope of 200 thousand meters in front and 300 thousand meters in depth six minutes prior to attack, and thus opened up a safe path for aviation troop penetration. In the beginning of the Gulf War, multi-national troops concentrated on information operation interference force by carrying out strong interference against Iraqi communications and radar and using F-117 stealth planes and precision-guided weapons to destroy the telecommunication building in Baghdad and radar control center 160 miles southwest of Baghdad to damage the Iraqi military command information system. During the Kosovo War, multi-national troops first attacked the Yugoslavian military command and control center in Belgrade. From here we can see that the procedure and target of regional war information operations under informationized conditions select the key and fatal parts to strike a deadly blow by focusing on the operation overall situation, surrounding the requirement on striking targets, and within the allowed space scope of the battlefield, which has an obvious difference from the front to rear gradual attacking method of traditional campaign tactics. (3) The nature of segregation in the information attack and defense main body. In the traditional operation form, an operation main body can carry out attack duty and also defense duty or it sometimes carries out attack duty and sometimes defense duty. Information operations also include information attack and information defense, but the attack mainly is the information attack activities of interfering, attacking, or destroying the enemy's information system and the defense mainly is the defensive activities of countering enemy information reconnaissance, counter electronic interference, and counter destruction. Therefore, joint campaign information operations are an information attack and defense operational form that consists of two mutually independent operational main bodies that are carried out at the same time. This unique operational form has formulated a uniformity in operational purpose as well as a contradiction in operational activities between the two main bodies – attack and defense, as they not only must fight shoulder to shoulder to seize information superiority but also closely coordinate with each other to prevent one's own being interfered.

Joint campaign information operations are generally divided into such information operations as island attack campaign information operations, joint fire power strike information operations, island blockade campaign information operations, anti air raid campaign information operations, and border defense campaign information operations.

Section 2: Main Measures of Joint Campaign Information Operations…12

Lenin pointed out that "an army cannot be in control of all fighting weapons and all fighting measures that the enemy has owned or will possibly own and anyone will

consider this to be foolish and even criminal."[4] Under the current situation, the informationized levels of our [China] operational opponent or potential opponent is very high and in comparison with ours, our opponent's information operational capability is clearly more superior; therefore, our keys to seize joint campaign initiative are to strengthen joint campaign information operational measure build-up and to accurately utilize every type of information operational measure. Joint campaign information operation measures mainly include electronic warfare, network warfare, and psychological warfare.

I. Electronic warfare…12

Electronic warfare was a new type of operational method that started in the early 20th century and was widely applied in the Second World War. Following the swift development and wide application in the military domain of electronic technology, electronic systems became an important pillar in supporting military operational systems, especially in the late 80s of the 20th century; the position and effectiveness of electronic warfare had further been raised. However, the definition on electronic warfare of all nations in the world is not the same and the focus of their debate concentrated mainly on the scope covered by electronic warfare. For example, the American military considers: "electronic warfare to be any military action that utilizes electromagnetic energy and directed energy controlling the electromagnetic frequency spectrum to attack the enemy's military."[5] The scope of this definition is very broad that includes not only soft strike but also hard destruction; while the scope of definition on electronic warfare of some other nations is comparatively narrower that is limited to only soft strike; for example, the electronic warfare of the Russian military only includes electronic reconnaissance and electronic suppression action on the enemy's electronic equipment and systems, as well as electronic defense of one's own electronic facilities.

Electronic warfare is electromagnetic struggle carried out by both opposing parties using electronic facilities or equipment and the purpose is to degrade or destroy the enemy's electronic facility effectiveness and at the same time, safeguard one's own electronic facilities to be fully effective. The future joint campaign battlefield will be an electromagnetic battlefield that reaches multi-dimensional spaces and is highly dependent on electronic facilities. In this battlefield, if it is not combined with electronic warfare measures, then it will be difficult for other operational measures to be effective. Regional wars that erupted in the 90s of the 20th century, such as the Gulf War and Kosovo War, sufficiently proved that electronic warfare had a very important meaning in seizing air dominance, sea dominance, and even dominance of the entire joint campaign battlefield. Therefore, electronic warfare will be one of the most important operational measures in

[4] *Complete Collection of Lenin*. Vol. 39, People's Publishing Press, 1985 Edition, p. 75.

[5] Regulations of American Military Joint Information Operations, 13 February 2006.

the joint campaign battlefield of the 21st century and will play a decisive role in gaining victory in war.

Electronic warfare includes mainly electronic reconnaissance, electronic attack, and electronic defense.

II. Network warfare…13

Network warfare is the sum total of various measures that one adopts in the computer network space by taking advantage of the security flaws of the enemy's network system to invade the enemy's computer network to steal, falsify, or damage the enemy's information and to decrease and damage the operational effectiveness of the enemy's computer networks; and at the same time, protect the security of one's own computer network for normal effectiveness.

After computer networks, which were developed in a short several decades, were applied to the military domain, the network space had become another brand new battlefield in military struggle. As a new operational method, network warfare has truly accomplished integrating the functions of single command, information sharing, timely discovery, and real-time destruction in the joint campaign battlefield; at the same time, following the constant increase of informationized levels in the battlefield, computer network warfare has also become an important component in information warfare and has been an important operation measure in seizing and maintaining control of information power in the battlefield. Network warfare is a double-point sword with two-sidedness as it is an important measure for strong nations to pursue the important measure of "defeating the opposition's military without fighting" and also an effective way for a weak nation to carry out an asymmetrical operation against a strong nation. The Kosovo War in 1999 was network warfare with real meaning in human history. During the war, even though NATO had air superiority and invaded the Yugoslavian alliance computer network system first, the smaller and weaker Yugoslavian alliance was able to confront the NATO force squarely and several times attacked the NATO "alliance action" computer network system in an organized way with very good results, causing the computer network on the American aircraft carrier "Roosevelt" to break down for three hours and the British meteorological service computer network station that NATO bombing relied on to be damaged seriously. Successful computer network warfare can make the enemy's advanced operation concept e difficult to implement and its weapon systems difficult to be effective, causing great weakening of the war potential and seriously affecting the war process. Sometimes computer network warfare can even be the major factor in deciding victory or defeat in war.

Network warfare mainly includes network reconnaissance, network attack, and network defense.

III. Psychological warfare…14

Psychological warfare is an operational action that uses all forms of information media, including all psychological factors such as thinking, emotion, reasoning, concept, point of view, and attitude as weapons to attack the enemy, causing the collapse of the enemy's will and spirit, confusion in its command and decision making, wavering confidence in operation, and decrease in combat force. Psychological warfare is divided into broad and narrow meanings. In the broad meaning, psychological warfare is psychological struggle to reach a specific goal and it mainly includes psychological struggle activity in politics, military, economy, culture, sport, and daily contact, so it covers a very broad scope. In the narrow meaning, psychological warfare is an operational activity that uses human psychology on aspects of politics, economy, and military as the operational purpose to reach a specific military goal; it influences human psychology through various measures so it would change and develop to a predetermined direction and create a psychological state that is beneficial to oneself and not beneficial to the enemy. The psychological warfare that we study generally is the one with the narrow meaning and its main task is to weaken and strike the enemy, solidify and strengthen ourselves, and reach the goal of "victory without fighting."

Following the constantly increasing level of military information, psychological warfare's position is heightened constantly on the joint campaign battlefield and its effectiveness is getting more and more important. In the Iraq War, the US military insisted on the tactics of "psychological offense being the best" and strengthened the application of psychological warfare, making psychological warfare action "all the way." Prior to the war, the US military gave wide publicity, claiming it will attack Baghdad from the north and west and covering its strategic intention of swift approach from the south, and it weakened the Iraqi main defensive military strength deployment. When the US military attacked Baghdad, it distributed large amounts of propaganda material and letters for inducing surrender to carry out propaganda to "overthrow Saddam" that greatly shook the Iraqi military mentality. At the end, the U.S. won the war with less cost and in a shorter time. Through the several regional wars that have erupted recently, all nations in the world gradually recognize that psychological warfare has the merit of decreasing war casualties and speeding up operational process, is an important measure in information operations, and also is an indispensable important measure in joint campaigns; therefore, they are paying more attention to the study of psychological warfare. Psychological warfare mainly includes psychological attack and psychological defense.

Section 3: Major Characteristics of Joint Campaign Information Operations…16

The characteristics of joint campaign information operations are the objective reflection of joint campaign information operation patterns and essential differences from other operational activities. To accurately promulgate and have an overall handle of the characteristics of joint campaign information operations are prerequisites to correctly carry out joint campaign information operations direction. The major characteristics of joint campaign information operations are as follows.

I. It is carried out prior to the other campaign activities and also through the entire campaign process…16

During joint campaign operation activities, information operations have already become a hallmark to initiate the entire joint campaign activity. Prior to the initiation of the joint campaign, both opposing parties put in all kinds of information reconnaissance force to carry out multi-positional reconnaissance and detection in order to obtain the opposition's campaign intelligence and further judge its combat capability, troop strength deployment, and operational plan to provide dependable basis for making the joint campaign decision and drawing up the operational plan. At the same time, they also try their best to stop the opposition from obtaining their own information in order to cover up their own action and intention. Most importantly is to use information attack activities such as electronic jamming, network infiltration, and psychological attack to damage the opposition's information system, disturb its military mentality, and achieve the goal of interrupting its preparation to carry out the operation. The primary target in joint campaign strike is also no longer the enemy's heavy military groups and artillery positions, but the enemy's information systems such as control, command, and communication in order to create conditions for seizing and maintaining control power of the battlefield and carrying out decisive combat. During the Gulf War, it was exactly because the US military had an absolute information superiority that its early on campaign activity was able to achieve the result of breaking down the Iraqi military command information system and thus laid the foundation for the smooth implementation of other operational activities.

On the one hand, the joint campaign operation pace is fast, operational activities are various, and the battlefield environment is complex, so the degree of its dependency on information is getting bigger and any operational activity cannot get away from the effective support and safeguard of information operational reconnaissance, information attack, and information defense activities. Whether in the action of seizing air dominance and sea dominance or in other operational activities, they must have the forceful support and coordination of information operations to be able to be carried out smoothly. On the other hand, information operations is also a type of operational activity mainly on "soft killing" and is very hard to basically completely take away the opposition's defensive capability, so in order to seize control of information power, one must have the coordination of regular fire force to destroy the enemy's information targets. Furthermore, as a "soft killing" activity, information operations also have a nature of effectiveness in a period of time; the seizing and maintaining of information superiority are relative and unstable and it is possible that one can always be in control of information superiority if one unceasingly carries out information operations surrounding the major operational activities during the entire operational process. It would determine the entire process in the joint campaign that information operations must go through; and even after the end of the visible battlefield confrontational activities, information operation activities are still continuously going on.

II. Information attack and defense are closely combined and the position of information attack is prominent…17

During a joint campaign, seizing information superiority depends on carrying out information operations with highly integrated attack and defense as the two are mutually dependent and none is dispensable. One is not able to take away and weaken the enemy's information control capability without information attack, cannot even talk about seizing control of information power, and information defense will always be in passive position and eventually it will possibly lose its meaning. At the same time, one cannot smoothly carry out information attack without information defense and one's own information control capability will gradually disappear. Therefore, in joint campaign information operations, information attack and information defense must be closely combined and none can be eliminated. Being different from the traditional operation method, information attack and information defense are not operational activities that are mutually taking place in turn and constantly interchanging as they must always accompany each other, be connected with each other, and cannot be separated.

Information attack is in a leading position in the struggle to seize control of information power. Information attack is an active attack on the enemy's information system using measures such as electromagnetic suppression, network attack, and fire power and military strength surprise attack. Information defense mainly utilizes activities such as safe security and protection of technology and programs to protect one's own information system from the enemy's jamming and damage and it almost has no effect on the enemy's information system; therefore, only information attack has the function to take away and weaken the enemy's ability to collect, transmit, and utilize information in the battlefield. One does not have to be in an overall advantageous position to carry out information attack, as the one in the disadvantageous position can also actively attack. The actual bodily destruction in information attack generally will cause the defender to have difficulty to recover in rather long period of time. The party that is attacked will also have difficulty to completely avoid seizing battlefield information superiority after suffering a sudden attack even if it has a comparatively full information defense preparation. These characteristics of information operations indicate that active attack and attack before the enemy does are the basic ways to seize and maintain information superiority. It determines that information attack has a decisive function in the struggle to seize and maintain control of information power.

III. Information operations strength is multiple and its command and coordination are complex…18

The information operation forces that participate in a joint campaign include not only direct subordinates of the theater but also subordinates of each operation group; not only the information operation force of the Army, Navy, and Air Force but also the information operations force of the Second Artillery and the Armed Police units; not only the information operations force within the organizational system but also the local non-organizational system information operations force participating in supporting frontline

operation; and not only the specialized information operations force with information attack activities as its major task but also the non-specialized information operations force.

Because all types of information operations activities often mutually affect and infiltrate each other, therefore, if the command and coordination are not well organized, then, not only would it be difficult to make information operations effective but also create serious effects on the normal operation of one's own electronic facilities and further affect the implementation of other operational activities; so one must comprehensively utilize the essence of these activities and maintain their high level of coordination to eliminate conflict and internal friction that may arise in order to achieve a mutually strengthening and mutually supporting operational result. For example, the combination of electromagnetic attack and precise substance destruction in a large area can basically damage the enemy's information system; under coordination with deception electromagnetic attack, deception psychological attack can more easily deceive the enemy's commander; and with the assistance of thorough defense, active attack is able to achieve the goal of not only damaging the enemy's information control capability but also maintaining one's own information control capability. Therefore, it is imperative that a joint campaign commander and his command organizations should carry out planning, coordination and control on all types of information operations forces with a macroscopic view and organize well the concerted coordination among all military services operation group information operation activities; organize well the coordination in information operations of major campaign directions and important campaign phases; organize well the coordination among the specialized information operations forces; and organize well the coordination among the electronic facility units (and branches), as well as the coordination between information operations activities and other campaign activities.

IV. Information operations integrates soft and hard in various measures…19

Information operations is a "dual-sided sword" that not only can carry out "soft strike" but also "hard destruction." The "soft strike" mainly depends on measures such as electronic jamming and computer virus attack, while "hard destruction" mainly depends on measures such as directed energy weapons, anti-radiation weapons, and fire power attack. In future joint campaign information operations, the gaining of battlefield superiority will, to a very large degree, depend on an organic combination of "soft strike" and "hard destruction" information operation activities. During the Gulf War, multi-national troops led by the U.S. at the same time carried out "soft strike" information operations, mainly electronic jamming, against Iraq and also carried out the unprecedented longest, largest-scale, strongest, and largest category "hard destruction" information operations activity against Iraq by using directed energy weapons such as cruise missiles and laser-guided bombs, anti-radiation weapons, and fire power strike. The US military's information operations activities with a combination of "soft strike" and "hard destruction" not only made the Iraqi military's key link in operational command and control and information systems to sink into the situation of breaking down and confusion at the beginning, but also its powers to collect, transmit, handle, and

utilize the battlefield information were taken away at the end and its all types of operational forces were like loose sand that could only be in a passive situation and take a beating.

Following the swift development in electronic technology, the information confrontational scope in a joint campaign under informationized conditions has already expanded to the new domains such as command information systems, computer networks, and space satellites and spacecraft and it not only has involved the highest command organs of the campaign large formations but also the tactical military units and branches and has infiltrated into the command and support systems of each military service and all types of weapon control systems. Therefore, on the information confrontational measure, there are not only communication, radar, and command information system confrontations but also computer virus confrontation; on the format of information confrontation, there are not only confrontations of information reconnaissance and anti-reconnaissance but also confrontation of information attack and counterattack and information destruction and counter-destruction. So, it has been determined that joint campaign information operations under informationized conditions will also be a multi-measure and multi-format operation.

V. Command information system is huge and complex and the task of information protection is large and difficult…20

The scope of a joint campaign is big with much war participating power; it has huge and complex command information system including information detection, information transmission, and decision-making on information handling; and it spreads over all domains in land, sea, air, and space. With the enemy laying out large numbers of remote sensing detection equipment in space, air, sea (under water) and land, the possibility of the joint campaign command information system's important activities such as assembly, maneuver, and deploy not being completely discovered by the enemy does not basically exist any longer. Facing the enemy's high-tech weaponry such as long-range precision guided ammunition, anti-radiation missiles, and electromagnetic pulse bombs and strike and damage of other operational activities; the difficulty for concealing the command information system's deployment and activities would be increased greatly. Wireless communication is the main method for operation command and control communications and the large amount of electromagnetic signals passing in the air would definitely be suppressed and jammed with electromagnetics in large scale by the enemy, making accurate and timely transmission of command and control information very difficult. Furthermore, due to the highly computerized and networking nature of the command information system, the enemy's network attack will cause great danger and damage to the information system, information operational process, and information security of the joint campaign military large formations and protection of computer networks will be one of the arduous tasks in information defense.

VI. Battlefield electromagnetic environment is complex and affects information operational activities greatly…21

In future joint campaigns, due to large amount utilization of electronic facilities and informationized weapons and equipment, battlefield electromagnetic radiation sources and electromagnetic signals will be highly concentrated, the categories of radiation signals will be many, and the electromagnetic environment will be very complex. Information operation is an operational activity carried out in the electromagnetic domain, so it will definitely be affected by the electromagnetic environment.

The complex electromagnetic environment increases the difficulty of information reconnaissance. With the concentrated use of a large amount of electronic facilities with highly concentrated electromagnetic signals and concentrated working frequencies, the ability of information reconnaissance to obtain the necessary intelligence information in the extremely crowded electromagnetic frequency spectrum will affect the ability of information receiving facilities in collecting, selecting, recognizing, and handling signals, making it difficult for us to effectively carry out reconnaissance positioning and friend or foe attributive recognition. In wartime, with the assistance of a strong enemy, the enemy military carries out key point information jamming against us or frequent changing of electronic facilities working frequency, making it difficult for us to effectively track the enemy's various types of electromagnetic signals and collect accurate intelligence information.

The operation of information attack measure is limited in a complex electromagnetic environment. With the increased number and variety of electronic facilities the enemy puts in the battlefield, we must also constantly increase the number and variety of electronic jamming facilities in order to carry out effective suppression against them. Allocation of a large amount of electronic facilities as well as the allocation of a large amount of electronic jamming facilities within a limited battlefield area may have serious mutual interference. Electromagnetic signal jamming under a complex electromagnetic environment affecting normal effectiveness of one's own electronic facilities has become a serious problem that affects operational effectiveness. Demand for electronic jamming technology and tactical utilization has become higher in order to lessen the effect on one's own.

The complex electromagnetic environment increases the arduousness of the information defense task. In the operation in a future complex electromagnetic environment, the enemy will have advanced information attack equipment and various information attack measures that will be a rather big threat to the utilization of our information system and informationized weapons and equipment. At the present time, the enemy's electronic warfare equipment basically covers the major operational frequency channels of our military wireless communications as well as warning, meteorological, gun-directing, and fire control radars and it is a very great threat to the utilization of our main operational use frequency equipment. In wartime, the involvement in electronic

warfare of a strong enemy will have even more measures, stronger capability, and greater influence. Faced with increasing variety and comprehensiveness of the enemy's information attack measures, our command information system protection may be in a passive position of being impossible to defend effectively and being put in a double squeeze, making the information defense task very arduous.

Section 4: The Position and Effectiveness of Joint Campaign Information Operations…22

For a rather long period of time since the presence of information operations, people's opinion of the position and effectiveness of information operations in war was not unanimous. The more common view was that information operations were an important combat support measure. Following the constant renewal in information operations equipment and the practice of several regional wars, people are paying more attention to the position and effectiveness of information operations in war and the traditional view has changed. Information operations is moving along the track and marching forward from low level to high level, from partial situation to overall situation, and from an operational support measure to operational attack and defense measures and is becoming an indispensable important measure in joint campaign operations under informationized conditions.

I. Information operations are an important component of joint campaign operational activities…22

In the future joint campaign battlefield, obtaining and maintaining air dominance, sea dominance, or land dominance must have information superiority as a prerequisite. In the early stage of a joint campaign, if a war participant could not effectively seize control of information power, then it would be very difficult to effectively expand and carry out the other operational activities as precision ammunition would not know the target, an airplane would be discovered by the opposition and destroyed, a ship would drift off course due to the navigational system being jammed, and the command information system would break down due to attacks on the network. On the contrary, if a war participant could seize battlefield information superiority, then the battlefield would become unidirectionally transparent, other types of operational action would develop orderly, and all types of operational activities would be in a beneficial position. During the Gulf War, multi-national troops carried out non-stop jamming on the Iraqi military command information system one week prior to the start of the war, carried out overall communication jamming 24 hours prior to action, and carried out large-scale, all-frequency channels blockage electronic suppression 5 hours prior to major attack. It was exactly how the US military depended on this continuous, highly efficient, fierce, active and high power information operation activity in the early stage to quickly take away the Iraqi military's control power of the battlefield, and thus paved a smooth path for the follow-up operational activities and laid a foundation for victory in the Iraq War. On the contrary, if the multi-national troops stopped information operation activities for a period

of time during the war, then the multi-national troops might be attacked by the Iraqi hiding or remaining fire power and suffer more losses.

Therefore, one can see that information operations is one of the most important actions in a joint campaign, causes decisive influence on the victory or defeat of war, and following the development of modern war, changes the informationized levels of war from low gradually to high.

II. Information operations are an effective way to seize joint campaign battlefield initiative…23

Initiative in the operation is the power of freedom and survival and the basis and prerequisite for winning operational victory. Victory and defeat in joint campaign operations, to a large degree, are determined by the control of the initiative in operational activities. The essence of information operations is a struggle between the opposite parties surrounding the seizing of the control power of information. The seizing of control power of information means that one can freely utilize information without the electromagnetic threat from the opposite party, and at the same time, take away the power of the opposite party to freely utilize information. Information operations can effectively restrict the effectiveness of the enemy's weapons and guarantee one's own large amount of weapons to effectively kill and injure the enemy's troops; it can clarify the enemy's deployment, fire power system, operational intent, and major direction to benefit one's own to purposefully organize joint campaign activities; it can cover up one's own deployment, operational intent, and fire power organization to avoid being damaged by the enemy's fire power; and it can break down the enemy's command, communication, and control systems so the enemy information cannot be transmitted, its operation troops have no command, and it cannot form an organized "fist." In joint campaign operations under future conditions, the party that is in control of information power will have great possibility to be in control of air dominance and sea dominance, further seize the war initiative, and strongly be in control of the war development situation to create the necessary condition for seizing war victory. The party that loses control of information power will sink into a passive condition of discontinued wireless communications, blinded radars, guided weapons losing control, optoelectronic facilities not functioning, and confused command and coordination and eventually lost control of the battlefield, leading to failure in war. One can see that seizing control of information power will win the initiative for joint campaign operational activities, guarantee the military operational; activities' power of freedom and survival, and lay a foundation and create a prerequisite condition for winning joint campaign operation victory. When one loses control of information power, one also loses the power of freedom and survival in operations and cannot do anything at all in seizing operational victory.

III. Information operations have become an indispensable operational measure in joint campaign operations…24

Following the development of modern information technology, information operations have broken through the traditional domains of wireless communications and radar confrontation and optoelectronic and acoustic confrontation and expanded to such aspects as network confrontation and psychological confrontation, developed from single measure confrontation to multi-measure comprehensive confrontation and from pure operation support measure to more direct attack and defense operation measure. Electronic warfare measures can be used to confront troops equipped with electronic information facilities (systems); network warfare measures can damage the enemy's network information system in the battlefield; electromagnetic pulse weapons can damage all kinds of electronic equipment and systems; psychological warfare measures can carry out psychological attack against the enemy; and successful utilization of anti-radiation missile, -laser, -particle beam and –high power microwave weapons will provide information operations with a hard killing capability to destroy all types of electronic facilities and systems. At the same time that information operations fiercely threaten and strike the enemy, it also bears the responsibility of preventing one's own information system and facilities from the enemy's information operations threat and strike. This peculiar attack and defense operational capability has made information operations to rise from an operation support measure in earlier campaigns to an indispensable important attack and defense operation measure with soft and hard killing capability in joint campaigns.

IV. Information operations capability has become an important mark of joint campaign operational capability…25

All sorts of weapons including artillery, tanks, airplanes, warships, and missiles utilized by modern military are equipped in different degree with electronic information facilities and command information system that commands modern military operations cannot even get away from electronic facilities. It is exactly because electronic facilities plays such an important role in a modern military that the level of information operations capability of a troop has a great effect on the winning and losing of joint operations. The regional wars since the 90s of the 20th century have made people deeply understand that a strong information operations capability is a prerequisite for winning modern war victory and information operations capability has become an important mark to measure the level of modern military joint campaign operation capability.

All nations in the world pay much attention to information operations and they spend a large amount of money for military expense, try their best to maintain quantitative and qualitative superiority in information operations equipment, and constantly improve their information operations organizational mechanism to strengthen information operations capability build-up. Information operations capability has become an important portion in various factors of foreign military combat force. Taking the US military as an example, after the 80s of the 20th century, its research budget on

information operations has been increasing greatly every year. In 1985, the total expense the U.S. spent on information operations was $56 hundred millions and after the 90s of the 20th century, its yearly actual expense on information technology and equipment could reach $400 – 500 hundred millions. The key point of US military current and future investment on information technology also concentrates on increasing command information system capability and precision attack capability. The Japanese military proposed to put information warfare capability along with fire power and maneuvering power as the third striking force. In recent years, the Chinese Military Commission headquarters has paid high attention to the build-up of information operations power and considers information operations power one of the Chinese military six major strategic forces.

Section 5: The Meaning in Joint Campaign Information Operations Study…26

Following the swift development of information technology, information operations position and effectiveness in joint campaigns have become more profound and the information operations issue is the key, difficult, and hot point issue in the leading edge of military theory study of all major militarily strong nations in the world currently. The study of joint campaign information operations has important meaning in further development and improvement of joint campaign information operations theory and for providing a basis for even more systematic and functioning to the joint campaign commanders and their command organization to organize and carry out information operations.

I. The requirements of joint campaign information operational implementation and development…26

After entering into the 21st century, all-military campaign information operations training and exercise activities are getting more popular; however, the retardation in theoretical instruction will definitely affect the increase in exercise results and standards and the implementation of joint campaign information operations has constantly asked for the earliest present of a joint campaign information operation theoretical system. The units (and branches) that are responsible for information attack tasks are in urgent need of campaign information operations attack theory to guide and regulate their activities in order to meet the requirements of information operations training; those that are responsible for information defense task are waiting for systematic and practical information defense theory to guide their actual activity in order to confront future information attack threats; joint campaign commanders and their command organizations are asking for the functional joint campaign information operations methods and principles for them to use; and all colleges and universities are urgently hoping to establish a joint campaign information operations theoretical system to meet the need for instruction and research in order to benefit the formation and development of information operation academic system. Doubtlessly, as long as there is requirement to practice joint campaign information operation, a theoretical system should be established and developed.

II. The important measures to speed up pushing for military struggle preparation…27

Facing the information age war challenge in the 21st century, we must study and understand the information operations thinking of the potential enemy's military strategy and analyze and clarify the electromagnetic environment in the surrounding of the future possible battlefield to greatly push for our military leap-over development and quicken well preparation for military struggle in order for our military operational activities to meet reality in the future battlefield.

The opposition in future war is an enemy with strong support and possessing obvious information superiority, and if we let it develop further its information superiority, then it would be impossible for our military to have "decisive victory in war." Therefore, we must target the peculiarity of military struggle preparation, deepen the study of joint campaign information operations issues, and understand very clearly the guiding ideas, basic principles, operation tasks, activity types, basic methods of operation, major measures, and countermeasures of our military joint campaign information operations in the future. The study and establishment of corresponding joint campaign information operations theory are beneficial to all military officers and men to further unify ideological understanding and establish the concept of using information to win; and they are also beneficial in guiding and towing the preparation and build-up of our military information operations and in seizing victory in future joint campaign information operations.

III. The urgent need to establish a joint campaign information operations theory with our military special characteristics…27

Currently, all major nations' military in the world place the basic point of military theoretical transformation on the study of informationized war operation theory. Such new concepts, new viewpoints, and new doctrine as "informationized warfare," "information warfare," "information operations," "command and control warfare," and "computer network warfare" are emerging in an endless stream and information operations theory has become a "commanding point" of campaign operations theory. One must raise the study of information operation theory to the position of strategy study in order to win future regional wars under informationized conditions.

However, because our military study of information operations is still in the transitional period from elementary study stage to high level study stage, there are still some issues that cannot be ignored, such as copying the information operations theory of foreign militaries, leaning more to study of information operations technical measures, and inadequate study of the harmonious nature of the combination between campaign and tactics. Therefore, we must target the existing shortage and problems in information operations theory study, use joint campaigns as the background, and seize and maintain control of information power in the battlefield as the goal to overall and systematically analyze and elaborate some key and difficult issues of future joint campaign information

operations and then provide methods and measures to adhere to and as basis in carrying out information operations training and activities to the joint campaign commanders and their command organizations and establish a joint campaign information operations theoretical system with our military special characteristics.

IV. Inner requirements to regulate joint campaign information operations training order…28

Our military joint campaign information operations theoretical study started considerably later; it was not until January 1999 that *Guidelines for Chinese People's Liberation Army Joint Campaigns* was issued to officially include information operation in the content of joint campaign operations. Through constant exploration in recent years, the understanding of information operations basic theory has gradually become unified and preliminarily formed an information operations theoretical system; however, the deficiency is that the transformation from information operations theory to training theory remains rather lagging behind. At present time, the gap in the study of all military information operations training theory is quite large and the troop information operations training has nothing to follow, does not know where to start, and cannot organize itself that it seriously restricts the enhancement of our military information operation capability. Strengthening the study of joint campaign information operation training and constantly raising the joint campaign information operations capability have become an urgent task in front of all military services.

Strengthening the study of joint campaign information operations theory is exactly in meeting the requirement of all military services' joint campaign information operations training and it not only is beneficial to regulating the joint campaign information operations training procedure, but also is beneficial to speeding up information operation capability build-up. It not only is able to fulfill the knowledge-seeking psychology in all levels unit and get rid of the blindness in joint campaign information operations training, but also to forcefully direct the troop's information operations training, push the enhancement of the overall information operations attainment, and promote the increase in quality of all sorts of information operations preparation and enhancement of the overall information operation capability.

V. Gradually integrate the requirements to understand joint campaign information operations ideology…29

Even though, as of now, our military has never carried out a joint campaign information operations in modern term, but the constant development in information technology and increase of social informationized levels have brought an understanding of information operations. Through several years of study, the whole military's understanding of information operations has been constantly deepening and they have a certain understanding of the concept and substance, responsibility and demand, and major actions of information operations, but their viewpoint is not entirely unanimous. Being a component of joint campaign operations theory, we must have a standardized

understanding of some major issues of the joint campaign information operations in order to form a unified will and to coordinate in unity to gain success in information operations.

Strengthening the study of joint campaign information operations theory can put together the information operations issues scattered in such domains as campaign, command, communication, and electronic countermeasure into one system and carry out a comprehensive study. It can reveal the common patterns of joint campaign information operations and provide method and strategy for utilizing these patterns to direct joint campaign information operations. It can grasp the essence of joint campaign information operations and have a handle of the substance of joint campaign information operations in order to create favorable conditions for achieving joint campaign initiative by unifying the ideological understanding of the commanders of war participating units in such aspects as guiding ideology, basic principles, responsibility and demand, and methods of operation, and measure and standardize activities according to a unified theoretical guidance to achieve concerted activities and integrated coordination, and formulate joint forces of all bodies to seize information superiority.

Chapter 2
Development History of Joint Campaign Information Operations…30

The emergence and development of information operations (IO) are the inevitable product of the wide-ranging application of information technology (IT) {*xinxi zuozhan*} in the military field {*lingyu*}. They are both the result of the pull of military needs {*xuqiu*} and the further propelling of technology, and also the result of the deepening of people's understanding of war activity laws {*zhanzheng huodong guilyu*} from [the viewpoint of] the relationship of science and technology (S&T) to war. Within past wars, although they did not put forth the IO of today, nonetheless an information trial of strength actually was present simultaneously with war, and developed to accompany the development of war. In studying [researching] {*yanjiu*} IO, one should understand the origins, formation, development, and motive factors {*dongyin*} in the development of IO.

Section 1: The Origins of Joint Campaign IO…30

With regard to the exploitation of information, it was already known in ancient times; but IO truly used at the campaign level {*zhanyi cengci*} is an event which occurred after the invention of modern communication means {*tongxin shouduan*}. It is generally held that joint campaign IO originated in the period from the late 19th century up to the beginning of the Second World War.

In the mid-to-late 19th century, the invention of the wired telegraph, telephone, and radio telegraph and their application on the battlefield enabled the realization of beyond-visual-range [BVR] {*chaoshiji*} long-distance real-time communication {*yuanjuli shishi tongxin*}, and realized **[end of page 30]** long-distance communication from warship {*junjian*} to warship, and from warship to land. People began to apply radio receivers to eavesdrop {*qieting*} on the enemy's wireless communication in order to acquire intelligence, and used radio transmitters {*fasheji*} to conduct jamming {*ganrao*} and sabotage {*pohuai*} of enemy communications. In particular, the wide-ranging application of Morse code {*mo'ersi dianma*} in the military made transmitting {*chuandi*} information among the armed forces even more convenient, speedier {*kuaijie*}, and higher in efficiency {*gaoxiao*}, so that even if two armed forces were separated by a hundred or even a thousand kilometers (km), they could still without the least effort {毫无费力地 *haowu feilidi*} communicate with one another, understand one another, and adjust-coordinate with one another {*huxiang xietiao*}. The invention of the telegraph and telephone extended man's auditory organs, and created "clairaudience" {*"shunfeng'er"*}, so that people were able to hear large amounts of information beyond their instinctive hearing; and the invention of the telescope and radar extended man's visual organs, and created "clairvoyance" {*"qianliyan"*}, so that people were able to acquire large amounts of information beyond their instinctive vision. Thus, IO within modern war, besides being carried out within humankind's natural instinctive information acquisition versus counter-acquisition, also exploits technical means and thus has unfolded {*zhankai*} information warfare [IW] {*xinxi duikang*}. In other words, IO, on the basis of intelligence warfare {*qingbaozhan*} and psychological warfare [PSYWAR]

{*xinlizhan*}, also has opened up a new operational field – electronic warfare [EW] {*dianzizhan*}.

In the Russo-Japanese War which broke out in 1904, the Russian military began to conduct electronic reconnaissance {*dianzi zhencha*} and electronic jamming {*dianzi ganrao*} against the Japanese military, and [thus] caused a setback to the Japanese warships' offensive {*jingong*}. This was the world's first implementation of EW {*dianzi duikang*} against an enemy; and even though {*jinguan*} it was something unconscious or a clouding of consciousness {*yishi mohu*}, it nonetheless drew open the curtain on modern campaign IO. In February 1904, Japan and Russia, to contend for dominance {*zhengduo… kongzhiquan*} over China's Northeast and the Korean Peninsula, initiated the world-shocking Russo-Japanese War. Within this war, the engaging sides {*jiaozhan shuangfang*} for the first time within operations employed radio to carry out signal communications {*tongxin lianluo*}. In the early period of the Russo-Japanese War, the Japanese military was preemptive {*xianfa zhiren*}, and took the initiative {*zhudong*}; but for a long time it was unable to capture Lushun seaport [Port Arthur]. The reason was that the Russian military's radio operators discovered that increases in the Japanese military's radio signals were portents of their attacks. Hence, the Russian military – via this important information on "increases in the Japanese military radio signals" – timely and accurately predicted {*zhunque yubao*} the Japanese military's attacks. This then was the emergence of electronic reconnaissance – the world's earliest exploitation of electromagnetic [EM] signals {*dianci xinhao*} to in advance issue warnings {*jingbao*} of an enemy's raids {*xiji*}. In March 1904, the Japanese Navy concentrated {*jizhong*} **[end of page 31]** firepower bombardments {*paoji*} of the Russian warships moored in the channels within Lushun harbor. Since the Japanese warships from overseas could not see the Russian warships moored within the harbor, their commander {*zhihuiguan*} decided to use one small destroyer {*xiaoxing quzhujian*}, moored at a certain advantageous location near the seacoast, to serve as an artillery observation post {*paobing guanchashao*}, to observe the impact points {*danzhuodian*} of the artillery shells {*paodan*} fired by the Japanese ships, and to use radio to carry out correction {*jiaozheng*} of the firing. At first, the Japanese naval gun {*jianpao*} [shells], just as if they had grown eyes, accurately flew toward their targets. However, a Russian radio operator within the Lushun seaport base {*jidi*} heard in his headset the communication signals between the Japanese ships. He had a bright idea {灵机一动 *lingji yidong*}, and pressed down on his telegraph transmitter {*fabaoji*} key, thinking in this manner to impede the communications among the Japanese ships. Sure enough, the Japanese military's wireless telegraphers suddenly heard very great static {*zayin*} between the transceivers {*diantai*}, and new firing target {*sheji mubiao*} information basically could not be transmitted, so that the Japanese military's artillery shells no longer could effectively hit their targets. This can be said to be the first radio communication jamming in the history of war. As of this point, the two basic essential factors {*yaosu*} of EW – electronic reconnaissance and electronic jamming – had been declared to the world, and EW had formally mounted the stage of war. During the following Russo-Japanese naval battle of Tsushima {对马海战 *duima haizhan*}, Japan's Combined Fleet {*lianhe jiandui*} employed electronic reconnaissance means to monitor {*jianting*} the Russian fleet's

radio/wireless communication {*wuxiandian tongxin*}, and grasped the movements {*dongxiang*} of the Russian fleet. In a predetermined sea zone {*yuding haiyu*} it set up an ambush attack {*shefu gongji*}, and via radio jamming facilities equipment {*ganrao shebei*}, it disturbed the Russian ships' signal communications, and achieved a major victory in which it sank 19 warships and captured 7 warships of the Russian fleet. These were the world's first IW activities {*xinxi duikang xingdong*} conducted by initiative-based application {*zhudong yunyong*} of modern IT, and also marked the formal emergence of EW.

During the First World War, IO with EW as the main content had its initial application within campaign operations. At that time, radio/wireless communication technology saw fairly universal application in the armed forces of the various nations, and in operational command {*zuozhan zhihui*} it brought into play ever more important roles {*zuoyong*}. Radio direction finders {*wuxiandian cexiangji*} entered real combat {*shizhan*}, electronic jamming began to be consciously applied in operations, and several of the main military powers began to organize and build EW units {*dianzizhan budui*}. In 1914, the British and French navies, with superior force-strength {*youshi bingli*} in the Mediterranean Sea, jointly carried out stalking {*weibu*} of Germany's fleet, and tried to annihilate {*jianmie*} it. Britain's cruiser {*xunyangjian*} *Gloucester* {"格林斯特" 号 *"gelinsite" hao*} **[end of page 32]** undertook {*danfu*} the mission of tailing the German warships; its goals {*mudi*} were to timely acquire the tracks {*xingzong*} of the German ships, and to use radio/wireless communication to timely report the activity situation of the German ships to the Royal Navy General Headquarters [HQ] {*zongbu*}, so as to organize force-strengths for carrying out surrounding and annihilation {围歼 *weijian*}. However, the British ships' signal communications were intercepted {*zhenting*} by the German ships, and their high-level radio/wireless communication also suffered intense electronic jamming by the German ships. Although the British several times changed their transmitting frequency, their communication always was jammed by a same-frequency-band {*tongyi pinduan*} signal sent out by the German ships, and they thus could not organize force-strengths to carry out surrounding and annihilation. The German ships seized this favorable opportunity for combat {*zhanji*}; suddenly turned about in navigation route {*hangxian*}; successfully shed the British fleet's encirclement, pursuit, obstruction, and interception {*weizhui dujie*}; and barely escaped from the jaws of death {虎口逃生 *hukou taosheng*}.

In August 1914, tsarist Russia's 650,000-man army {*dajun*}, divided into the 1st and 2nd Group Armies {*jituanjun*}, mounted a large-scale offensive {*daju jingong*} against Germany. In the northeastern part of the battle lines, Germany only had the 8th Group Army to resist the Russian military's offensive, so the circumstances {形势 *xingshi*} were extremely unfavorable to the German military. Just at that time, the Russian military, which lacked elementary knowledge of the new electronic technology {*dianzi jishu*}, used plain code {*mingma*} to send out a copy of a top-secret telegram {*juemi dianbao*} on the force-strength disposition {*bingli bushu*} and operational plans {*zuozhan jihua*}, and this important telegram to its surprise was intercepted {*qieting*} by a German military radio station {*wuxiandian tai*}. The German military, via analysis and

study {*fenxi yanjiu*} of the telegram's content, discovered that there was a gap more than 100 km wide between the Russian military's two group armies, and that the complementation {*peihe*} between these two group armies of the Russian military was very poor. Hence, the German military first concentrated its main force and launched a fierce offensive against the Russian military's 2nd Group Army; and when it learned that the Russian military's 1st Group Army had no intention of carrying out reinforcement {*zengyuan*} of the 2nd Group Army, the German military then felt relieved and boldly used a force-strength of only one division to contain {*qianzhi*} the 24 divisions of the Russian military's 1st Group Army, and thus used most portions of its force-strengths to surround and annihilate the 2nd Group Army. As a result, the German military very rapidly annihilated the Russian military's 2nd Group Army, and afterward in turn concentrated its force-strengths and annihilated the Russian military's 1st Group Army. In this campaign, the German military, by only paying the price of 10,000 casualties {*shangwang*}, thus killed, wounded, and captured almost 300,000 men of the Russian military. Although the means of EW during the First World War were extremely simple, and although the quantity used, scale, and goals which needed to be achieved all were very limited, nonetheless the enormous might {*weili*} which EW displayed shocked people, and impelled several nations' militaries to begin developing {*yanzhi*} specialized {*zhuanmen*} **[end of page 33]** EW equipment {*dianzizhan zhuangbei*}, and to organize and build professional EW units {*zhuanyede dianzizhan budui*}.

Although EW {*dianzi duikang*} commenced during the First World War, nonetheless the technology still was not mature, its application within campaigns similarly was not widespread, the confrontational means {*duikang shouduan*} were unitary, and the modes {*fangshi*} were relatively simple. Interception {*zhenting*} and direction finding {*cexiang*} were taken as primary, with occasional use of electronic jamming; these lacked professional facilities equipment for EW, and were limited to being within the scope of communications countermeasures [CCM] {*tongxin duikang*}, so that the effects were limited. Thus, EW still had not attracted universal attention. Moreover, just in terms of the joint campaign itself, this phase similarly was still not fully mature, and IO even more had not become an important component {*zucheng bufen*} of the joint campaign.

Section 2: The Formation of Joint Campaign IO…34

The formative period of joint campaign IO mainly signifies the period from the Second World War up to just before the Persian Gulf War {*haiwan zhanzheng*}. IW technology {*xinxizhan jishu*} saw development, special-purpose IW facilities equipment {*xinxi duikang shebei*} was fielded to the units, a small number of IO units were created, and IO started to become an important component of joint operations. The formative period of joint campaign IO can be divided into two phases: the World War II era and the postwar period up to the Persian Gulf War.

I. Joint campaign IO in the World War II era…34

During World War II, due to war needs and requirements {*xuyao*}, the opposing sides {*didui shuangfang*} put great energy into research and development [R&D] {*yanfa*} of navigation {*daohang*} and radar technologies, and unfolded {*zhankai*} sharp EW centering on their application. Radar countermeasures [RCM] {*leida duikang*}, CCM, electro-optical [E-O] countermeasures {*guangdian duikang*}, and hydroacoustic countermeasures {*shuisheng duikang*} together constituted the basic content of EW, and established the position {*diwei*} of EW within war. Nations one after another launched {*kaizhan*} research into EW technology, and constantly created special-purpose EW equipment to throw into real combat. Use of radio and radar enabled the operational activities {*zuozhan xingdong*} in the air and on the ground (at sea) to be adjusted-coordinated consistently. Air dominance/supremacy {*zhikongquan*} became an important assurance of land dominance {*zhiluquan*} and sea dominance {*zhihaiquan*}, **[end of page 34]** and there emerged new operational patterns {*zuozhan yangshi*} such as EW.

By 1935 and 1936, Britain, the U.S., and Germany had produced {*shengchan*} radar systems {*leida xitong*}. In 1935, Britain [first] produced air defense radar {*fangkong leida*} which could detect aircraft, and this precipitated the debut of radar jamming instrument equipment {*leida ganrao qicai*}. In 1940, the Wehrmacht [German military], in order to bomb Britain, built a series of "Lorenz" {"洛仑兹" *"luolunzi"*} navigation systems in northern France. The British military, in order to jam the Lorenz systems, developed the "Meacon" {"米康" *"mikang"*} analog jamming system {*moni ganrao xitong*}. The Wehrmacht also successively developed the "LFF" {"拉芬" *"lafen"*} [Landefunkfeuer] and "Benito" {"贝尼托" *"beinituo"*} navigation systems, and the British military also developed the "Bromide" {"布罗米德" *"buluomide"*}, "Domino" {"多米诺" *"duominuo"*}, and other special-purpose navigation jamming instrument equipment and their countermeasures. In 1940-1941, the British military built special-purpose radar electronic jamming systems such as "Aspirin" {"阿斯匹林" *"asipilin"*} and "Bromide" {"澳化剂" *"aohuaji"*}, conducted jamming against the Wehrmacht's radar, and [thus] caused the Wehrmacht's air defense system of systems [SoS] {*fangkong tixi*} to further fall into a passive situation {*beidong jumian*}. At the same time, the British military developed passive jamming {*wuyuan ganrao*} instrument equipment – [metal] chaff {*jinshu botiao*} – and when the Anglo-American joint forces {*lianjun*} conducted large-scale air raids on Hamburg, Germany, they for the first time employed passive jamming chaff, totaling 2.5 million cassettes. This caused the Wehrmacht to falsely count the 790 British and American bombers {*hongzhaji*} participating in the air raids as several thousand such planes.

During the war, following on the needs and requirements of air combat {*kongzhan*} and sea combat {*haizhan*}, RCM were formed and saw rapid development. From the viewpoint of CCM aspects, ground jamming facilities equipment experienced fairly great development, and dozens of types of specialized CCM facilities equipment emerged. At the same time, airborne communication jammers {*jizaide tongxin ganraoji*}

also emerged. As for the RCM aspects, besides active jamming {*youyuan ganrao*}, passive jamming instrument equipment such as chaff and angular reflectors {*jiaofansheqi*} was widely applied on the battlefield, and specialized aircraft for conducting jamming against radar appeared; camouflage and deception {*weizhuang, qipian*} were widely applied within campaign and combat activity {*zhandou xingdong*}, and became important support measures within campaigns and battles.[6]

During the Normandy landing campaign {*denglu zhanyi*}, the synthetic [comprehensive] application {*zonghe yunyong*} of many types of instrument equipment and multiple means within EW activities brought into play extremely important roles in terms of achieving the surprise quality {*turanxing*} in the campaign and seizing the battlefield initiative {*zhudongquan*}. The "[Operation] Fortitude, North" {"北方坚韧" *"beifang jianren"*} deception plan which the US-British allied forces {*mengjun*} implemented in northern Europe contained a Wehrmacht force-strength of 10-some divisions, so that it did not dare to transfer them to France **[end of page 35]** to participate in anti-landing {*kangdenglu*} operations. The "[Operation] Quicksilver" {*"shuiyin"*} deception plan implemented at Dover created in the Wehrmacht the false impression that the allied forces were about to conduct a large-scale landing in the Calais area {*diqu*}, and caused the Wehrmacht to produce a mistaken assessment of the allied forces' main landing direction {*zhuyao denglu fangxiang*}. At the same time, the allied forces synthetically applied multiple EW measures to conduct jamming and deception against the Wehrmacht, and successfully provided important support for the landing. Within the operation, accompanying the main attack formations {*zhugong biandui*}, they conducted active jamming {*jiji ganrao*} of the Wehrmacht's radar and communication in the Normandy direction, and shortened its reconnaissance distance {*zhencha juli*} and detection probability {*faxian gailyu*} in the main landing direction. At the same time, in the Calais area, the allied forces used aircraft for large-quantity release of jamming chaff {*ganrao botiao*} and mounted angular reflectors on motor launches {*qiting*}; this jammed and deceived the Wehrmacht's radar, and created the false impression that an allied forces large-scale fleet was launching an offensive. These measures successfully deceived the Wehrmacht, and created extremely favorable conditions for achieving success in the landing campaign.

II. Joint campaign IO from the end of World War II up to the Persian Gulf War…36

Since the end of World War II, although no more world wars have occurred, nonetheless no fewer than 100-some local wars and armed conflicts {*wuzhuang chongtu*} of various natures, scale, and patterns have occurred. All of these local wars to different

[6] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

degrees have reflected several characteristics {*tedian*} of modern war, and even have revealed the embryonic form {雏形 *chuxing*} of future informationized wars {*xinxihua zhanzheng*}. Among these local wars and conflicts, those having a fairly great influence are the Korean War {*chaoxian zhanzheng*}, the Vietnam War, the [four] Mideast Wars, the Falklands War {马岛战争 *madao zhanzheng*}, and the War in Lebanon. Within these wars, the position and role {*diwei zuoyong*} of IO have been prominent, and its scope and influence have been extremely wide-ranging; this has attracted maximum attention from the armed forces of nations around the world. IO theory has begun to become an attention point for research, and the application of computers in the military has greatly boosted the capability for IO. Large quantities of informationized equipment {*xinxihua zhuangbei*} are being developed {*yanzhi*} for application in the armed forces, and IO is starting to consciously become a relatively independent phase to be implemented within military activities.

Beginning in the 1960s, communication, radar, and E-O technologies saw full-speed development, and the large-quantity application of guided weapons {*zhidao wuqi*} simultaneously became the main means of attack. This impelled the all-around development of IO technology; various types of special-purpose EW aircraft, **[end of page 36]** electronic reconnaissance satellites {*dianzi zhencha weixing*}, expendable jamming facilities equipment {*touzhishi ganrao shebei*}, anti-radiation missiles [ARMs] {*fanfushe daodan*}, and similar EW weaponry {*dianzi duikang bingqi*} were successively thrown into operations, and brought into play a clear combat power "multiplier" {*zhandouli "beizengqi"*} role within modern operations. During the Vietnam War, North Vietnam for the first time within anti-air raid operations {*fankongxi zuozhan*} adopted brand-new air defense missile [ADM] weaponry {*fangkong daodan bingqi*}; this altered the past operational model {*zuozhan moshi*} in which aircraft were first and antiaircraft guns {*gaopao*} were second within struggle {*douzheng*} against air-raiding aircraft, so that ADMs became the basic strengths {*liliang*} for defense {*fangyu*}. The hit probability {*mingzhonglyu*} of this type of radar-guided ADM generally could reach 95%. However, after the US military employed airborne radar warning {*jizai leida gaojing*} and electronic jamming, the hit probability then markedly decreased, to 1.4% - 2%. The 1973 Fourth Mideast War [or "Yom Kippur War"] even more involved an electronic battlefield for repeated trials of strength between the EW strengths of the engaging sides. Since the Egyptians had fielded "SAM-6" {"*samu-6"*} missiles guided by new-frequency-band gun aiming radar {*paomiao leida*} and continuous wave [CW] radar {*lianxubo leida*}, and "SAM-7" infrared [IR] guided missiles {*hongwai zhidaode daodan*} equipped with IR-jam-resistant filter lenses {*kanghongwai ganrao lyubojing*}, the Israeli military did not have a clear understanding of timely reconnaissance and [thus] did not adopt the corresponding resistance measures, so that at the beginning of open hostilities {开战伊始 *kaizhan yishi*} it suffered huge losses.

Beginning in the 1970s, following on the large-quantity application of IT in the military field, advanced weapons and equipment {*wuqi zhuangbei*} within the armed forces were already informationized. There appeared large quantities of high-tech operational platforms, precision-guided munitions [PGMs] {*jingque zhidao danyao*}, EW

weapons {*dianzizhan wuqi*}, night vision instrument equipment {*yeshi qicai*}, and full-dimensional {*quanfangwei*}, full-time-domain {*quanshiyu*}, all-weather reconnaissance, surveillance {*jianshi*}, detection {*tance*}, navigation, and positioning systems {*dingwei xitong*}. In particular, the use of command information systems {*zhihui xinxi xitong*} fused on-battlefield intelligence reconnaissance {*qingbao zhencha*}, communication, command, control, and strike into an organic whole {*yiti*}, so that the position of information within war had a qualitative leap. Information became the "leading factor {*zhudao yinsu*} in victory or defeat in war," and enabled the emergence of joint campaign IO to become possible. In particular, CCM systems and integrated RCM systems {*zonghe leida duikang xitong*} have been formed as triads {*sanwei yiti*} composed of EW reconnaissance, survey [measurement] {*celiang*}, and jamming facilities equipment. The prominent role they brought into play within war and the enormous influence they produced played extremely important driving roles in the all-around development of EW. In the Bekaa Valley battle between Israel and Syria in 1982, to understand how Israel **[end of page 37]** only took 6 minutes to destroy in a stroke 19 of Syria's SAM-6 missiles, and how in air combat it shot down 79 Soviet-made MiG aircraft of Syria's at a minuscule price, the main reason is that prior to combat, Israel – by stealing and releasing into air unpiloted electronic decoy aircraft {*wuren jiashide dianzi youer feiji*} – ascertained the tactical technical parameters {*zhanshu jishu canshu*} of the Syrian military's ADM radar, and in a manner having a directed [focused] quality {*you zhenduixing di*}, as a result implemented electronic jamming against that radar.

Section 3: The Development of Joint Campaign IO…38

This period mainly signifies that from the Persian Gulf War to the present, joint campaign IO from theory to practice has seen major developments. In particular, during the Gulf War and Kosovo War, it acquired all-around demonstration, its important position and role won universal acknowledgement {举世公认 *jushi gongren*}, and IO capability became an important standard {*biaozhun*} for judging the combat power of a nation's armed forces.

During the 1991 Gulf War, the electronic struggle – with electronic reconnaissance versus counter-reconnaissance {*fanzhencha*}, jamming versus counter-jamming {*fanganrao*}, destruction versus counter-destruction {*fancuihui*}, and control versus counter-control {*fankongzhi*} as its main content—was unusually sharp and complex, and became within war the content of a trial of strength with material destruction {*wuzhi cuihui*} and counter-destruction having the same level of importance. As far back as the period before the start of the war, the US military had dispositioned {*bushu*} 10-some photographic and electronic reconnaissance satellites in the space over the Persian Gulf, and conducted full-dimensional, uninterrupted {*bujianduan*} rigorous surveillance {*yanmi jianshi*} of Iraq. Also, the Coalition Forces {*duoguo budui*} had in three directions—Israel, Turkey, and Saudi Arabia {沙特 *shate*} – dispositioned a group of airborne electronic reconnaissance jamming aircraft {*kongzhong dianzi zhencha ganrao feiji*}, including the EA-6B, EF-111A, EC-130, and F-4G, which had electronic and IR jamming facilities equipment and omnidirectional warning systems {*quanxiang*

gaojing xitong}, as well as 8 EW intelligence battalions {*dianzizhan qingbao ying*} and 5-7 EW intelligence companies {*dianzizhan qingbao lian*} equipped with radar transmitting positioning and reconnaissance systems {*leida fashe dingwei zhencha xitong*}, radar reconnaissance receiving systems, communication intercept and direction-finding systems {*tongxin zhenshou cexiang xitong*}, and communication jamming systems. [Coalition Forces thus] completely seized EM dominance {*zhidianciquan*} in the theater space {*zhanqu kongjian*}. **[end of page 38]** After the start of Operation "Desert Storm" {*"shamo fengbao" xingdong*}, the US military conducted an electronic offensive, code named Operation "White Snow" {*"baixue" xingdong*}, in EM space. This involved large-area, long-lasting jamming of the Iraqi military's communication systems, and led to the Iraqi side's command and control [C2] systems {*zhihui kongzhi xitong*} being completely paralyzed {*tanhuan*}, its radar screens being covered with snowflakes, and its radio stations {*guangbo diantai*} for a while being out of order {失常 *shichang*}. Within the air raid process, the Coalition Forces used AGM-88A anti-radar missiles to accurately strike at the Iraqi side's air defense systems: as long as an Iraqi radar was turned on, within a few seconds the anti-radar missiles were able to accurately destroy it. These powerful attacks in the battlefield information field, with EW as the main form {形式 *xingshi*}, ensured that the Coalition Forces all along seized the battlefield initiative. During the Gulf War, the degree of ferocity in the Coalition Forces' electronic attacks and the enormous role brought into play by them were things never experienced within past wars.

The Kosovo War pushed IO toward a new development phase. During the Kosovo War, the US military, besides applying traditional EW means, also widely employed a good many new-concept weapons {*xin gainian wuqi*} to execute crushing strikes {*huimiexing daji*} on the information systems and electric power systems of the Federal Republic of Yugoslavia [FRY] {南联盟 *nan lian meng*}. For example, it repeatedly used conventional EM pulse bombs [E-bombs] {*dianci maichong dan*}, leading to "large-area paralysis" of the FRY's electronic information systems. The US military also for the first time used carbon-fiber graphite bombs {*tan xianwei shimo zhadan*} to specially strike at and sabotage the FRY's electric power systems. After this type of bomb exploded in the air, it could produce large quantities of long thin carbon-fiber strips; once these strips fell onto high-voltage transmission lines or transformers, they could create short-circuits, and thus incinerate the power transmission equipment and paralyze the electric power system. It is thus clear that new-concept weapons became a new means of EW.

In [the history of] human war, the Kosovo War was the first large-scale war reported over the Internet {*hulianwang*}. As soon as the war began, NATO exploited the Internet, and repeatedly at great length {连篇累牍 *lianpian leidu*} reported the so-called true state of the war {*zhanzheng zhenxiang*}, to prepare the public {鸣锣开道 *mingluo kaidao*} for the war's actions {*xingjing*}. Simultaneously with this, the FRY, in order to counterattack {*fanji*} NATO's propaganda warfare, also exploited Internet sites {*zhandian*} to constantly transmit its own voice to the entire world. Via the Internet, it in good time transmitted NATO's savage acts {*baoxing*} in the war onto networks, and sent

out reconnaissance information consistent with the identifying characteristics {*shibie biaoshi*} of its information and intelligence systems. **[end of page 39]** At the same time, the FRY fabricated its own battlefield information and projected false intelligence {*jiaqingbao*} to deceive the coming enemy. The FRY military also fully exploited NATO's abundant Internet information resources, over the 'Net collected information resources on the weapons and equipment of all NATO nations which participated in the air raid activities, and thus provided powerful assisting support {*zhiyuan*} for its anti-air raid operations. In addition, ever since NATO had first launched air raids against the FRY, NATO's official website {*guanfang wangzhan*} had constantly suffered attacks by computer hackers {*heike*}. Several computer warriors {计算机斗士 *jisuanji doushi*} of the FRY exploited computer software, sneaked into NATO's server connecting to the Internet, and within a short time injected several thousand illicit pieces of information, which caused problems such as the NATO website appearing to be blocked {*duse*} and user access {*yonghu fangwen*} having difficulty. NATO's internal {*neibu*} e-mail system also was honored with hacker [intrusions], and every day it received more than 2000 "electronic bombs" {*"dianzi zhadan"*} of illicit mail. According to a NATO spokesperson who declined to reveal his or her name, during the war some of NATO's computer websites had suffered heavy losses {*zhongchuang*} inflicted by computer viruses {*jisuanji bingdu*} coming from the FRY. News reports said that FRY computer experts, under the assistance of Russian hackers, had once attacked into the C2 system of the US Navy's *Nimitz* aircraft carrier {*"Nimizi" hao hangkong mujian*}, and caused its communication to be out of order {*shiling*} for up to several hours. In addition, the US FBI's website and other government websites also suffered the attacks of hackers, causing several websites for long periods to be in a closed status {*zhuangtai*}. The great network war {*wangluo dazhan*} which broke out during the Kosovo War broke new records in the operational patterns within humankind's recorded history of war. The adoption of multiple means to implement PSYWAR was another prominent feature of the Kosovo War. The U.S.-led NATO's tactics {*celue*} of "troops who subdue the enemy without battle" {"不战而屈人之兵" *"buzhan er quren zhibing"*} already had its proponents {情有独钟 *qingyou duzhong*}, who fully recognized the principle of "to take the enemy by force, first capture their hearts" {"夺人先夺心" *"duoren xian duoxin"*}, and placed PSYWAR in an important position. At the beginning of April [1999], Britain's Foreign Secretary [Robin] Cook {库克 *kuke*} in a public address said that the FRY's First Lady Mila and her children had quietly left Yugoslavia and gone to another country. This sensational {耸人听闻 *songren tingwen*} news was transmitted to Yugoslavia, and naturally played a certain role in confusing the people. This is because if it were really just as Cook had said, then it meant that Milosevic {米洛舍维奇 *miluosheweiqi*} had already made preparations for defeat. On 27 May, International Criminal Tribunal for the Former Yugoslavia [ICTY] {前南国际战犯法庭 *qiannan guoji zhanfan fating*} inspector [Louise] Arbour {阿尔切尔 *aerqieer*} announced that she was prosecuting for war crimes Milosevic and four other former Yugoslavian leaders. **[end of page 40]** This also was a new product of the PSYWAR cooked up {*paozhi*} by the leaders of the U.S., UK, and other nations. Its intent {*yitu*} was unusually clear: to isolate the FRY leaders and to create in them enormous psychological fright {*xinli konghuang*}. When carrying out the campaign operations-research-based planning {*zhanyi chouhua*},

they considered PSYWAR content and objectives {*mubiao*} within it. At the start of the air raids, almost 100 personnel of the 4th PSYWAR Group {*dadui*} [4th PSYOP Group] subordinate to the US Special Operations Command [SOCOM] {*tezhong zuozhan silingbu*} at top speed were moved from the U.S. to Italy. Some [members] even penetrated deep into the Kosovar "Albanian Liberation Army's" [KLA's] {科索沃 "阿族解放军" *kesuowo "azu jiefangjun"*} controlled area, drew up {*niding*} PSYWAR activities courses of action [COAs] {*xingdong fang'an*}, and conducted a multilevel, full-dimensional PSYWAR offensive {*gongshi*} against Yugoslavia. First, they set up the "NATO PSYWAR Broadcast TV Station." This group recommended that the US Air Force [USAF] dispatch 6 EC-130 aircraft. At an altitude of 10,000 meters, group personnel exploited the medium-wave and FM bands {*zhongbu, tiaopin boduan*} used by Yugoslav State radio and TV stations, and in the Serbian language broadcast PSYWAR information. Next, together with the NATO International Military Staff HQ {*canmoubu*} Public Relations Department, as well as related intelligence institutions, they joined hands to prepare PSYWAR propaganda materials and false information {*jiaxinxi*}, which they widely sent out to the mass media. In addition, based on PSYWAR tenets, they recommended strikes on susceptible targets {*mingan mubiao*}, including the Yugoslavian president's official residence and bombing of the Yugoslavian electric power and water supply systems. In order to keep the Yugoslavian people from timely obtaining true information on the air raids and anti-air raid [activities], NATO before dawn on 23 April bombed the Yugoslav State TV station, and on the 27th it used missiles to destroy the TV broadcasting tower mounted at the top of the Serbian Socialist Party's HQ building.

The main characteristics of IO at this time were as follows: first is that IO had become an important component of the joint campaign. IO had become the "first gun" fired in an independent phase of the joint campaign, even before the launch of the joint campaign's overall activities {*zongti xingdong*}; it moreover penetrated from start to finish of the entire campaign. This [point] had a typical embodiment within the Persian Gulf War and Kosovo War. Second is that IO technology had produced qualitative leaps: various types of IO weapons had emerged in an endless stream {层出不穷 *cengchu buqiong*}, and informationized weapons had become "multipliers" of combat power. During the Kosovo War, the sorties into action {*chudongde jiaci*} by the NATO armed forces' EW aircraft constituted more than 40% of the total number of aircraft sent into action. In addition, the "decoys" towed by aircraft conducted air raids, and also acquitted themselves splendidly during the war. One new type of IO weapon – the EMP bomb [E-bomb] – [**end of page 41]** saw application in real combat. Third is the maturation of IO thought and the proposal of integrated {*wanzheng*} IO theory, as well as the establishment of the corresponding institutions. Before the Gulf War, studies of IO only involved individual efforts {*xingwei*} sporadically carried out by theorists within and outside of the militaries of various nations; but after this war, they then became studies by the nation's leading [researchers] {*zhudao*} and efforts of practice. This phase of research on IO further deepened, and also further deepened studies on fighting methods {*zhanfa*} for IO.

In 1992, the US Department of Defense issued *DoD Directive* {*zhiling*} *3600.1—Information Warfare* {*xinxizhan*}, which began to study IO theory in key point based, phase-by-phase manner {*you zhongdian, fenjieduan di*}, and developed IW capabilities. The fiscal year 1995 US *Defense Report* carried out a delimiting {*jieding*} of IO, and the fiscal year 1996 *Defense Report* at fairly great length discussed IO issues. The US military's *Joint Vision 2010* {*2010 nian lianhe gouxiang*} and its accompanying full set of {*peitao*} trans-century long-range plans {*guihua*} for the various services and arms {*junbingzhong*} all at very great length discussed the importance and main content of IO. In 1993, DoD took the lead in carrying out structural adjustment {*tiaozheng*} of its directly subordinate institutions, and clarified the duties {*zhize*} of each department in terms of developing IO capabilities. In 1994, it established an Information Systems Security Center {*xinxi xitong anquan zhongxin*}, Joint Staff C2 Warfare Center {*lianhe canmoubu zhihui kongzhizhan zhongxin*}, and Joint Staff IO Bureau {*lianhe canmoubu xinxi zuozhan ju*}. The US Army, Navy, and Air Force respectively established the corresponding IO institutions, and issued the corresponding operational regulations {*zuozhan tiaoling*}.

At the same time, all nations of Western Europe – and in particular Britain, France, Germany, and Italy – also were actively conducting studies on IO and open-up development [exploitation] {*kaifa*} of IO capabilities, developing informationized equipment, and building digitized units {*shuzihua budui*} and digitized battlefields. France and Italy were exploiting {*kaifa*} "intelligence and command systems" used for tri-service joint operations {*sanjun lianhe zuozhan*}; they also were placing key point investment in building of theater-level command information system {*zhanquji zhihui xinxi xitong*} projects, such as NATO airborne C2 systems {*kongzhong zhihui kongzhi xitong*}. The British Army {*lujun*} invested large amounts of funds {*zijin*} in building an integrated system {*yitihua xitong*} for command HQ {*silingbu*} work, C2, logistics {*houfang qinwu*}, and combat support {*zhandou zhiyuan*}. This system would join more than 400 users and 56 stations {*zhandian*} in the armed forces of the UK and Germany. The US military held that from the viewpoint of the theoretical development of IO, **[end of page 42]** first was for "electronic warfare" to be developed into "C2 warfare," and then to evolve into "information operations." C2 warfare on the battlefield would be the entire basis for IO, while EW would be the basic pillar for C2 warfare.

Section 4: Motive Factors in the Development of Joint Campaign IO…43

Although IO has developed following on the emergence of war, nonetheless for a long time it was not at all recognized by people; and only with the recent several local wars was it able to attract the wide-ranging attention of people. The main reasons for this include the following several points.

I. The inevitable product of IT application…43

The swift development of IT and its wide-ranging application in the military field thus led to IO within modern war being further developed. The development of IT

promoted the informatization {*xinxihua*} of the armed forces' internal weapons and equipment and the informatization of command modes {*zhihui fangshi*}. Since the 1990s, the development of weapons and equipment among nations around the world already has begun to convert to applying modern IT in order to transform and provide an informationized degree for weapons and equipment. Informationized munitions {*danyao*}, informationized operational platforms, military-use intelligent robots, individual digitized equipment {*danbing shuzihua zhuangbei*}, and networked {*wangluohua*} C2 systems have attained very great development. This has caused early warning detection {*yujing tance*}, C2, intelligence communication, firepower strike, battlefield maneuver {*jidong*}, and logistics support to be formed into a closely coordinated {*miqie xietong*} integrated operational SoS {*yitihua zuozhan tixi*}. The development of armed forces informatization has maximally boosted the armed forces' C2 capability, but also is exposing lethal weak points. The reliance of the armed forces on networked information systems is growing ever greater, and at the same time it also is becoming a weak vital site {*yaohai*} for enemy attack. Sabotaging or destroying important network systems enables creating lethal strikes against the adversary. This then requires that the armed forces not only must strengthen {*jiaqiang*} friendly information defense {*jifangde xinxi fangyu*}, to ensure the security of friendly information and information systems; they also must actively implement **[end of page 43]** information offense {*xinxi jingong*}, to sabotage the enemy's information and information systems. Hence, the position of IO is growing ever higher, and its influence on the progress {*jincheng*} and outcome {*jieju*} of campaign combat {*zhanyi zhandou*} is growing ever greater.

II. The inevitable choices for the changes in strategic needs {*zhanlue xuqiu*}…44

Since the entry into the 21st century, all of the world's main military powers have taken as the objective gaining victory in wars of the Information Age, and have unfolded even sharper arms races. Developing informationized operations weapons and equipment and building of informationized units have become the inevitable choices for all nations' military strategic readjustment {*junshi zhanlue tiaozheng*}. Around the world, which nation would think it will go and fight a large-scale war of the type such as the two world wars? Traditional large formations {*da bingtuan*} and large campaigns {*da zhanyi*} no longer find favor. Having gone through analysis of the Cold War and deep thinking on the pain and suffering [of large-scale wars], people have begun to gradually shift their attention onto small-scale wars {*xiaozhan*}, and to seek deterrent means {*weishe shouduan*} and operational capabilities {*zuozhan nengli*} more suited to the circumstances of today's world and to fairly low-level conflicts. This form, IO, is relatively adapted to this need. The EW and computer network warfare {*jisuanji wangluozhan*} trial of strength in the EM field and the struggle on computer fluorescent screens cannot be like two armies facing one another {*liangjun duizhen*}, depleting {*xiaohao*} even more resources and creating even more personnel casualties. Informationized weapons have the capability for striking point targets {*dianzhuang mubiao*}, and their kill area {*shashang mianji*} can be restricted to within a certain scope. They are also beneficial to reducing the necessary casualties, and to gaining a great victory at a small cost. Great reduction in casualties is one of the important motive factors

in the development of IO. Hence, under the enormous driving force of strategic needs, IO is seeing rapid, all-around development.

III. The necessary result of the world's Revolution in Military Affairs [RMA] {*junshi geming*}…44

Since the debut of firearms {*rebingqi*}, which have undergone development changes of almost a thousand years, their tactical technical characteristics {战技性能 *zhan ji xingneng*} already have approached the physical limits. The greatest feature of the RMA {*xin junshi geming*} is its wide-ranging employment of IT. The result is that the range (of fire) {*shecheng*}, navigation range {*hangcheng*}, speed, and similar high-tech characteristic performance indices {*xingneng zhibiao*} of the various types of weapons and operational platforms which have approached the physical limits now are seeing new development and breakthroughs. The application of IT in the military has brought along enormous benefit, and has changed the past traditional development mentality {*silu*} of purely pursuing the scale of war {*zhanzheng guimo*} and damage effects {*huishang xiaoguo*}. In terms of weapons and equipment **[end of page 44]** technical composition, it has constantly increased the information processing capability of weapons systems; realized informatization, smartness {*zhinenghua*}, and networking {*wangluohua*} of weapons systems; and brought forth IT-centered weapons systems such as information munitions {*xinxi danyao*}, informationized operational platforms, individual digitized equipment, and command information systems. Thus, it has laid the material foundation for implementing IO. If we can say that the RMA {*junshi jishu geming*} has given "new life" to the physical limits of weapons and equipment, then the "new life" in the weapons and equipment physical limits in turn have caused the theory of war {*zhanzheng lilun*} and its patterns and means to undergo qualitative changes, and will hasten the birth of a new type of operation mode {*zuozhan fangshi*} – the birth of information operations.

IV. The inevitable result of rethinking of war goals {*zhanzheng mudi*} and means…45

Since ancient times, the goals of war have been to wipe out {*xiaomie*} the enemy and to preserve oneself. To achieve these goals, for the past almost 200 years, humankind all along has been pursuing boosts in the destructive power {*pohuaili*} of war and weapons, and ultimately is developing nuclear, biological, and chemical [NBC] {*he, sheng, hua*} weapons of mass destruction [WMD] {*daguimo shashang pohuaixing wuqi*}. However, the maximum boosts in the destructive power of weapons contrarily have formed the factor which restricts their use. As a result, people now are seeking more "civilized" means of war, which not only reduce the casualties and destruction within war, but also can similarly achieve the goals of war. Following on the full-speed development of IT and the wide-ranging application of information weapons systems {*xinxi wuqi xitong*}, people have realized new achievements in the exploration {*tansuo*} of operational modes. In other words, via IO, they are changing the direction of the spearhead of war from attacking cities and pillaging territory {攻城掠地 *gongcheng luedi*} to [focusing on] the adversary's cognitive systems {*renzhi xitong*}: the

information systems for command, communication, control, computers, and intelligence [C4I], and the enemy's decision-making groups {*juece qunti*}. Via operational means with information capability {*xinxineng*} as the main one, they ultimately attack the enemy's knowledge {*renshi*} and conviction {*xinnian*}, forcing the enemy to renounce the desire to resist {*dikang yiyuan*} and thus halt operations, and achieving the war goal of "controlling the enemy and preserving oneself." Thus, IO has become a new operational pattern for achieving this war goal. The remarkable expression of IO during the Persian Gulf War has deepened people's understanding {*renshi*} of the superiority {*youyuexing*} of this operational pattern within practice, and this outcome has further catalyzed the formation of this pattern known as information operations. **[end of page 45; end of chapter]**

This page intentionally left blank.

Chapter 3
Guidance Thought {*zhidao sixiang*} and Principles of Joint Campaign Information Operations…46

Joint campaign information operations (IO) guidance thought and the principles which should be followed are the basic foundation for operations-research-based planning {*chouhua*} and conducting of joint campaign IO. Hence, determining the correct guidance thought and basic principles is of extremely important significance for setting the correct IO resolution {*dingxia... juexin*} and for organizing and implementing IO activities {*xingdong*}, and even for the peacetime building of command and armed forces informatization {*zhihui jundui xinxihua*}.

Section 1: Guidance Thought…46

Joint campaign IO guidance thought is the concentrated {*jizhong*} embodiment of the characteristics and laws {*tedian guilyu*} of IO, and is the basic foundation for all levels of command of and organizing of IO. The determination of IO guidance thought not only must comply with the characteristics and laws of IO, but also must comply with our military's reality. In particular, within future military struggle {*douzheng*}, our military's IO will be faced with the challenge of a hostile side's {*didui fang*} powerful IO strengths {*liliang*}. Only when we best the enemy in planning {高敌一筹 *gaodi yichou*} in terms of operational guidance {*zuozhan zhidao*} can we seize and maintain the initiative {*zhudongquan*} in IO.

The organizing and implementing of joint campaign IO must take as guidance Mao Zedong's military thought, Deng Xiaoping's thought on armed forces building in the new era, Jiang Zemin's national defense and armed forces building {*jundui jianshe*} thought, and **[end of page 46]** Hu Jintao's important descriptions of national defense and armed forces building under the new circumstances {形势 *xingshi*}. They must focus on effectively carrying out our military's historic mission in the new century and new phase; take the new-era military strategic concept {*junshi zhanlue fangzhen*} as the foundation; and abide by the basic guidance thought of "active offense {*jiji jingong*}, sabotaging networks and severing the chain {破网断链 *powang duanlian*}, thorough protection, and seizing and maintaining local information dominance {*jubu zhixinxiquan*}." [This means] concentrating elite {*jingrui*} IO strengths, and with active initiative {*jiji zhudong*}, using information offensive activities {*xinxi jingong xingdong*} to seize the advantage of the first opportunity {*xianji zhili*}; placing key points {*zhongdian*} on striking and sabotaging the enemy's reconnaissance and early warning net {*zhencha yujing wang*}, command communication net {*zhihui tongxin wang*}, and civilian information installations {*sheshi*} supporting {*zhicheng*} the enemy's operational activities {*zuozhan xingdong*}, and on severing the enemy intelligence information chain {*qingbao xinxi lian*}, command information chain {*zhihui xinxi lian*}, and weapons control information chain {*wuqi kongzhi xinxi lian*}; and thoroughly organizing information defense {*xinxi fangyu*}, ensuring that our information systems {*xinxi xitong*} correctly bring into play

their effectiveness {*xiaoneng*} and [ensuring] operational information security [INFOSEC] {*xinxi anquan*}, and struggling hard to seize and maintain information dominance in the joint campaign's main operational direction {*zhuyao zuozhan fangxiang*}, main battlefield, main phases, and critical time segments {*guanjian shijie*}, so as to create favorable conditions for the success of the joint campaign.

I. Basic connotations…47

"Active offense" is an objective requirement {*yaoqiu*} for IO in modern war, and is the basic avenue for achieving IO goals {*mudi*}. Active offense, within the entire process of joint campaigns, means seizing various favorable time opportunities {时机 *shiji*}, adopting active IO activities, [seizing the] first opportunity to subdue the enemy {*xianji zhidi*}, and struggling hard for the initiative. Active offense is something determined by the special quality {*teshuxing*} of the information field {*lingyu*}; that is, it has reflected the general laws of initiative-based offense which operations emphasize under informationized {*xinxihua*} conditions. Even more important is that it has grasped the special requirements of struggle in the information field. In future military struggle, a powerful enemy inevitably will intervene {介入 *jieru*}, and use its own superior strengths {*youshi liliang*} to conduct powerful information attacks {*xinxi jingong*}. If the weaker {*ruoshi*} side has a passive {*beidong*} information defense, that could make it impossible to defend effectively {防不胜防 *fangbu shengfang*}, and that side all along would be in a passive position. If one wants the initiative, one must with initiative launch an attack {*zhudong chuji*}. Offense is the best defense; without offensive there is no initiative, and without initiative one cannot gain victory {*zhisheng*}. During the Kosovo War, the Federal Republic of Yugoslavia [FRY] {南联盟 *nanlianmeng*}, even though {*jinguan*} it was in [the position of] information inferiority {*xinxi lieshi*}, nonetheless adopted active offense methods, and achieved the combat results {*zhanguo*} of shooting down an F-117 stealth fighter {*yinxing zhandouji*} and several cruise missiles {*xunhang daodan*}. On the other hand, during the Persian Gulf War {*haiwan zhanzheng*}, Iraq blindly [adopted] a passive defense {*xiaoji fangyu*}; via measures such as camouflage and concealment {*weizhuang, yinbi*}, **[end of page 47]** although it reduced some losses, it nonetheless achieved absolutely no combat results to speak of.

"Sabotaging networks and severing the chain" are the critical links {*guanjian huanjie*} of IO. Even if it is a powerful enemy having information superiority {*xinxi youshi*}, its information systems still are its "soft rib." "Sabotaging networks and severing the chain" means the need to seize favorable opportunities for combat {*zhanji*}; select strike directions and strike nodes {*jiedian*}; and synthetically [comprehensively] apply {*zonghe yunyong*} means such as electronic jamming {*dianzi ganrao*}, network attacks {*wangluo gongji*}, anti-radiation destruction {*fanfushe cuihui*}, and special sabotage-raids {*tezhong poxi*} – to paralyze {*tanhuan*} the adversary's information systems, weaken the adversary's information attack capability, and to the maximum extent cause the enemy's networks to be sabotaged and their chains to be severed, his command to go out of control {*shikong*}, his activities to be imbalanced {*shitiao*}, his weapons to lose accuracy {失准 *shizhun*}, and his psychology to go out of balance

{*shiheng*}. During the Kosovo War, the US-led NATO units {*budui*} all along had powerful information superiority, but the FRY actively organized information attacks, and for a time caused the NATO general headquarters {*zongbu*} computer network server to be congested {*zuse*}, leading to a crash. Hence, "sabotaging networks and severing the chain" are the critical links for weakening the enemy's information superiority, degrading his integrated-whole operational capability {*zhengti zuozhan nengli*}, and changing the IO strength comparison {*liliang duibi*}, and are inevitable choices for seizing local information dominance.

"Rigorous protection" {*"yanmi fanghu"*} is an important means for protecting friendly {*jifang*} information systems from loss. Within joint campaigns, since the information systems are huge and distributed over a wide area, with interconnection and intercommunication {*hulian hutong*}, the systems are relatively vulnerable {*cuiruo*}; and as long as the critical nodes {*guanjian jiedian*} of an information system meet with enemy jamming, sabotage, and/or destruction, the entire system then can be paralyzed. In order to boost survivability {*shengcun nengli*}, [we] must adopt rigorous protection measures, to guard against attack and defense going out of balance {*gongfang shiheng*}, and against attending to one while losing sight of the other {顾此失彼 *guci shibi*}.

"Seizing and maintaining local information dominance" is the ultimate goal of IO. In terms of the overall situation of the campaign {*zhanyi quanju*}, seizing and maintaining local information dominance within the foreseeable future will be things difficult to realize. Hence, seizing and maintaining local information dominance in the campaign's main direction {*zhuyao fangxiang*}, critical nodes, and important areas {*diqu*} then will become the focal points of contention {*zhengduo jiaodian*} in future joint campaign IO. This then requires that we must, on the basis of active offense and rigorous protection, concentrate the use {*jizhong shiyong*} of various types of IO strengths and means, and – in the campaign operations' main direction, important zones {*diyu*}, and critical time segments – to the maximum extent strip away the adversary's use and dominance {*kongzhiquan*} of information. At the same time, we must adopt effective measures to support {*baozhang*} the normal operation of friendly information systems, **[end of page 48]** so as to create the conditions for seizing the initiative in the joint campaign.[7]

The four aspects of IO guidance thought are a tightly connected {*jinmi lianxi*} organic integrated whole {*youji zhengti*}. "Active offense" is the basic avenue for IO, "sabotaging networks and severing the chain" are the critical links of IO, "rigorous

[7] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

protection" is the assurance of the security of friendly IO, and "seizing and maintaining local information dominance" are the ultimate goals of IO.

II. Basis for establishment…49

Joint campaign IO guidance thought serves as rational knowledge {*lixing renshi*} of the characteristics and laws of IO under certain historical conditions, and should have a solid basis in practice and a scientific theoretical foundation. The guidance thought of "active offense, sabotaging networks and severing the chain, thorough [sic] protection, and seizing and maintaining local information dominance" is something put forth to focus on objective reality {*keguan shiji*} of the current state {*xianzhuang*} of our military's IO strengths, as well as of the opponent's situation. It not only complies with the general guidance laws {*zhidao guilyu*} of modern joint campaigns, but also complies with the special {*teshu*} guidance laws of our military's future joint campaign IO command. It possesses fairly strong epochal features {*shidai tezheng*} and a very strong scientific quality {*kexuexing*}, directed [focused] quality {*zhenduixing*}, and guidance quality {*zhidaoxing*}.

(1) Characteristics of IO strength employment

In future local wars under informationized conditions {*xinxihua tiaojianxia jubu zhanzheng*}, the joint campaign IO strength composition {*liliang zucheng*} will have contained Army, Navy, Air Force, Second Artillery, and armed police units {*wujing budui*}; IO activities will involve network space, psychological space, electromagnetic [EM] space {*dianci kongjian*}, and operational platforms spread all over land bases {*luji*}, sea bases {*haiji*}, air bases {*kongji*}, and outer space {*taikong*}, as well as under water; and the IO targets/objectives {*mubiao*} will be numerous, and their objects {*duixiang*} complex. The joint campaign IO strengths not only must carry out confrontation {*duikang*} with the information systems of the enemy facing our joint campaign large formations {*zhanyi juntuan*}, but also must jam and sabotage the strategic information systems {*zhanlue xinxi xitong*} on which his operations are dependent, and furthermore must sabotage the civilian information installations which support {*zhicheng*} his operations. Faced with such strenuous IO missions {*xinxi zuozhan renwu*}, solely relying on professional IO strengths {*zhuanye xinxi zuozhan liliang*} will make it difficult to fulfill them. [We] must synthetically apply various types of operational strengths; achieve a mutual combination of "soft kill" {*"ruan shashang"*} and "hard destruction" {*"ying cuihui"*} strengths, and a mutual combination of professional and non-professional strengths; thoroughly adjust-coordinate {*xietiao*} **[end of page 49]** the IO activities of each space, each type of IO strength, and each direction; and see that they act in concert with one another {彼此呼应 *bici huying*} and are organically complementary {*peihe*}. In this way, [we] will be able to realize the goals of joint campaign IO, and to seize and maintain local information dominance.

(2) Basic law of IO taking offense as primary

The establishment of any one type of operational guidance thought always must consider the basic characteristics and inherent laws of the operational activities which it guides. In future local wars under informationized conditions, a powerful enemy's intervention in the information field will be unavoidable; and faced with the enemy's powerful information attacks, a passive information defense inevitably will [make it] impossible to defend effectively. Hence, active offense is the key to weakening the enemy's information superiority. In an enemy having information superiority, the information systems precisely will be his weak points. If [we] can apply powerful information attack means to effectively sabotage the information systems on which the enemy heavily relies, then his high-tech superiority with information superiority as its core may then be greatly weakened. Just as in the nuclear era, when only relying on the "three defenses" {*"sanfang"*} [protection against nuclear, biological, and chemical threats] could not break through the enemy's nuclear blackmail {*he ezha*}, and only by having developed offensive nuclear weapons {*jingongxing he wuqi*} and having formed powerful nuclear deterrence {*he weishe*} were [we] able to keep the enemy from daring to rashly use nuclear weapons – similarly, only by energetically developing IO means, and forming effective information warfare [IW] deterrence {*xinxizhan weishe*} and real combat capability {*shizhan nengli*}, can [we] force the enemy to dare not act rashly and blindly {轻举妄动 *qingju wangdong*}. Although in terms of overall strength comparison {*zongti liliang duibi*} our profession IO strengths are in the inferior position, nonetheless we have adequate IO potential {*qianli*}, have rich high-tech talent superiority {*rencai youshi*}, have flexible {*linghuo jidong*} people's war {*renmin zhanzheng*} IO fighting methods {*zhanfa*}, and have constantly developing IO strengths and means. All of these have provided assurances of implementing active information offense.

(3) Objective current state where the enemy is strong and we are weak in IO strengths

Subjective guidance complying with objective reality is a basic requirement for establishing operational guidance thought. In future local wars under informationized conditions, the quantity of our military's IO strengths will be limited, the equipment gap {*zhuangbei chaju*} will be fairly large, and real combat experience will be insufficient. The building of specialized psychological warfare [PSYWAR] {*xinlizhan*} and computer network warfare [CNW] {*jisuanji wangluozhan*} strengths is just getting started, and the situation where the enemy is strong and we are weak in IO strengths will **[end of page 50]** be present for a long period, so the desire to seize and maintain information dominance in terms of the overall situation of the campaign will be very difficult [to realize]. However, at the same time, we also have mastered some "assassin's mace" weapons {*"shashoujian" wuqi*} in the information field, have [realized] fairly many achievements in terms of theoretical innovation of IO fighting methods, and have possessed the capability for seizing and maintaining local information dominance. This objective situation is an important basis which must be given close attention in establishing our military's joint campaign IO guidance thought. Concentrating the

employment of elite {*jingrui*} IO strengths in these two main operational patterns {*zuozhan yangshi*}, EW and CNW; conducting active initiative-based information offensive operational activities, to bring into play the backbone role {*zuoyong*} of our military's limited IO strengths; striving to change weakness into strength; using strong points to attack weak points {以长击短 *yichang jiduan*}; taking the initiative; and positioning the campaign IO goal on seizing local information dominance – these precisely are based on the basic reality of the enemy being strong while we are weak in future joint campaign IO strengths, and are grounded in operations under the most complex and most difficult conditions.

Hence, we must want to establish the thought of "seizing and maintaining local information dominance;" on the basis of "active offense" and "rigorous protection," concentrate the employment of various IO strengths and means in the campaign operations' main direction, important zones, and critical time segments; take seizing and maintaining local information superiority as the direct operational goal; execute powerful information attacks against the enemy's main information systems; and to the maximum extent strip away his use and dominance of information. At the same time, [we must] adopt effective measures to support the normal operation of friendly information systems, so as to create favorable conditions for seizing the initiative in joint campaign operations.

(4) Experience in the practice {*shijian jingyan*} of IO

Theory originates in practice. IO theory – and especially IO guidance thought serving as the core content of IO theory – is no exception. With regard to this type of entirely new operational activities known as IO, our military, although lacking in operational practice, nonetheless has felt its way {*mosuo*} and amassed certain training experience {*xunlian jingyan*}. In recent years, our military has regarded IO as important content in joint campaign exercises {*yanxi*}, repeatedly has organized specialized campaign EW exercises {*dianzi duikang yanxi*} **[end of page 51]** and CNW exercises, and in depth has launched theoretical research {*kaizhan lilun yanjiu*}; these have realized a good many valuable achievements. What must be seen is that within the high-tech local wars since the Persian Gulf War, foreign militaries have acquired much experience in the successful practice of joint campaign IO. Examples include active offense, preemption {*xianfa zhiren*}, tight combination {*jinmi jiehe*} of attack and defense activities {*gongfang xingdong*}, simultaneous use of "soft" and "hard" means, mutual complementation of technology and tactics {*jishu zhanshu xianghu peihe*}, and implementation of integrated operations {*yitihua zuozhan*}. All these are useful references for establishing our military's joint campaign IO guidance thought. The IO guidance thought put forth in this text specifically focuses on absorbing the experience of our military's training exercises and the achievements of theoretical research. In a manner providing analysis and distinction, it draws upon the foreign militaries' operational experience; tightly combines this with our military's reality and the needs and requirements of future military struggle; carries out abstraction {*chouxiang*} of the core content of operational guidance, including the main patterns and main-force activities which should be adopted in joint campaign IO and the basic goals to be achieved; and as

much as possible uses simple and easily understood language to summarize and form [this IO guidance thought]. This then organically unifies the means and the goals. That is, it has emphasized the core thought and important content, has avoided devoting attention to all aspects of the matter {面面俱到 *mianmian judao*}, and also is easy to understand and grasp; it has the distinct characteristics our military.

(5) Basic guidance thought and principles of the joint campaign

Joint campaign IO is an important component {*zucheng bufen*} of a joint campaign. Hence, joint campaign IO guidance thought must take the joint campaign's basic guidance thought and principles as its theoretical foundation. Our military's *Joint Campaign Guidelines* {*lianhe zhanyi gangyao*} has established the joint campaign basic guidance thought of "integrated-whole operations and key point strikes {*zhengti zuozhan, zhongdian daji*}," and has put forth 10 principles, including "knowing the enemy and knowing yourself {知彼知己 *zhibi zhiji*}, and striving for subjective guidance complying with objective reality." Its mental essence {*jingshen shizhi*} is to set out from the actual situation of the enemy and friendly sides {*diwo shuangfang*} and the battlefield's objective environment; fully bring into play the integrated-whole operational might {*zhengti zuozhan weili*} of all services and arms {*zhu junbingzhong*}, as well as of other participating strengths {*canzhan liliang*}; and apply flexible, effective fighting methods to execute key point strikes against the vital site positions {*yaohai buwei*} and weak links of the enemy's operational system of systems [SoS] {*zuozhan tixi*}. This is the direct theoretical foundation for establishing our military's joint campaign IO guidance thought. The IO guidance thought put forth in this text specifically focuses on **[end of page 52]** all-around embodiment of joint campaign basic guidance thought and principles, and tightly combines these with IO characteristics, to creatively implement and apply them. The grounding in the joint campaign's overall situation, as emphasized by this guidance thought, takes seizing of local information dominance as creating the conditions for success in the joint campaign. It actively implements offense, executes key point strikes against the enemy's command and control [C2] systems {*zhihui kongzhi xitong*}, carries out rigorous protection of our military's information systems, and works hard to realize the tight combination of information offense and information defense. It takes EW and CNW as the leading factors {*zhudao*}, mainly uses the various types of IO strengths in these two patterns, synthetically applies the various patterns of IO, and fully brings into play the basic connotations, such as integrated-whole operational might. All this is tightly linked up {*xianjie*} with the joint campaign's basic guidance thought and principles, and brought together with them for a thorough understanding of the subject {融会贯通 *ronghui guantong*}; and its mental essence is entirely consistent.

III. Issues which should be grasped in implementing and applying joint campaign IO guidance thought…53

(1) Establishing new concepts {*guannian*}

Establishing the joint campaign IO guidance thought of "active offense, sabotaging networks and the chain, thorough protection, and seizing and maintaining local information dominance" means adapting to the new circumstances of IO and to the needs and requirements of new missions, and is the result of fully advancing with the times {与时俱进 *yushi jujin*} and of theoretical innovation. To implement and apply this guidance thought, [we] must establish new concepts, and constantly deepen the understanding of the important position and important role of IO. In the transitional period {*zhuanxing qi*} of our military's dual historic mission to complete mechanization and building of informatization, and to realize modern leap-forward development {*kuayueshi fazhan*}, if our thought concepts are not developed and not renewed, and remain stuck in the old thinking mode {*siwei moshi*} of mechanized and semi-mechanized war, then we cannot calmly respond to the enormous conflicts and profound changes which IO has introduced into modern war. Before us are the urgent needs and requirements to break free from the shackles of old thought and old concepts, and to establish new concepts for IO. First is the need to establish the concept that information is an important combat power {*zhandouli*}. In this period, the practice of several local wars fully proves that information already has become an important factor {*yinsu*} in armed forces building and development, and is a "multiplier" {*"beizengqi"*} of combat power. Having deviated from information, force-strengths {*bingli*}, firepower, and maneuver {*jidong*} then cannot be effectively **[end of page 53]** organized and implemented, and will have even more difficulty in bringing into play their roles and forming integrated-whole operational capability. Second is the need to establish the concept of information going ahead of the rest {先行 *xianxing*}. As the saying goes: food and fodder should go before troops and horses {兵马未动, 粮草先行 *bingma weidong, liangcao xianxing*} [i.e., proper preparations should be made in advance]. Today, then, is [the time for] information to go ahead of the rest, and IO already has become the "forerunner" {*"xianxingzhe"*} of modern local war. Information preparations going before those of the other operational essential factors {*zuozhan yaosu*}, viz., force-strengths, firepower, and maneuver, and IO activities going before other operational activities, already have become a [sic] prominent characteristic of modern high-tech local war. Third is the need to establish the concept that information superiority is the operational initiative {*zuozhan zhudongquan*}. Information superiority is the most fundamental, most central operational superiority, and by having information superiority, quantitative [numerical] superiority, scale superiority {*guimo youshi*}, and tempero-spatial superiority {*shikong youshi*} then have significance. It is just as comrade Jiang Zemin once pointed out: "Within local war, without information dominance, one cannot then speak of sea dominance {*zhihaiquan*} [command of the seas] and air dominance/supremacy {*zhikongquan*}." Without effective control of and the free use of information, [we] similarly cannot seize and maintain the initiative in joint campaigns.

(2) Correctly processing three relationships

To implement and apply joint campaign IO guidance thought, [we] must properly process several important relationship issues relating to the overall situation of the campaign and its outcome {*jieju*}. Among these it is especially necessary to devote attention to and properly process relationships in three respects: "between the integrated whole and the parts {*jubu*}, between offense and defense, and between centralization and decentralization {*jizhong yu fensan*}." First is properly processing the relationship between the integrated whole and the parts. Within joint campaigns, on one hand, [we] must properly process the relationship of the IO part to the joint campaign's integrated whole. IO serves as an important component of joint campaigns, and must be subordinate to and in the service of the overall situation of the entire campaign. On the other hand, [we] also must properly process the relationship of the various components of IO to the integrated whole of IO. IO is composed of essential factors, including multiple strengths, patterns, and activities; so [we] not only must lay stress on the special quality of these essential factors and bring into play their important roles, but also must ensure that all of them can be unfolded {*zhankai*} to center around this integrated whole of IO. Second is properly processing the relationship of offense to defense. The active offense required by joint campaign IO guidance thought is established on the basis of thorough defense, and is not at all a belittling and/or exclusion {*paichi*} of information defense. The actual situation of our military's IO strengths and weapons and equipment **[end of page 54]** has determined that offense and defense must be tightly combined, and that we cannot purely emphasize information offense, nor can we passively organize information defense. Instead, [we] should accomplish having defense within offense, having offense within defense, using offense to assist defense, and using defense to promote offense, to jointly bring into play their proper operational effectiveness {*zuozhan xiaoneng*} for seizing campaign local information dominance. Third is properly processing the relationship of centralization to decentralization. Centralization and decentralization within joint campaign IO are a unity of opposites {*duili tongyi*}. Our military's IO strengths are weak, and in terms of organizational structure {*bianzhi*} they are also decentralized in units of the various services and arms. During operations, they must be unified in organization and centralized in employment, to form fists. Centralization mainly signifies the centralization of IO capabilities, and is not the centralization of force-strengths and weapons {*bingli bingqi*} in the traditional sense. At the same time, [we] also must consider timely decentralized disposition {*fensan bushu*} of IO strengths and equipment, and avoid centralized deployment {*jizhong peizhi*} due to spatial [needs], which would create losses in strengths.

(3) Laying stress on bringing into play the integrated-whole might of IO

The ultimate implementation of joint campaign IO guidance thought must rely on the effective bringing into play of the integrated-whole might among all strengths, all means, all activities, and all battlefields of IO. To this end, [we] should conscientiously do a good job of combination in the following four respects. First is the mutual combination of professional strengths and nonprofessional strengths. The EW and

network warfare [CNW] units (elements) {*bu (fen) dui*} subordinate to the Army, Navy, Air Force, and Second Artillery Corps are professional strengths engaged in IO, and are the main body of IO; they undertake {*danfu*} the main operational missions {*zuozhan renwu*} and bring into play the main roles. Beyond these, the IO nonprofessional strengths also are indispensable important components of the integrated-whole strength of IO. The two each have their strong points, and they should be organically combined, for integrated-whole subduing of the enemy {*zhengti zhidi*}. Second is the mutual combination of armed forces strengths will local strengths {*difang liliang*}. Joint campaign IO requires the energetic support {*zhichi*} and active participation of the masses. This special operational field has provided a vast battlefield for local information strengths to participate in and bring into play a role. IO should fully exploit the information resources of the local rich talent, technology, and installations, and in different operational spaces {*zuozhan kongjian*} and fields realize integrated operations {*yiti zuozhan*} of military-local information strengths {*jundi xinxi liliang*}. Third is the mutual combination of IO activities and other operational activities. **[end of page 55]** Within joint campaigns, the tight connection between IO and other operational activities is an organic integrated whole. The combining of IO activities together with other operational activities must, while actively bringing into play the might of the IO activities themselves, excel at drawing aid from the effects of other operational activities, so as to serve the seizing of campaign local information dominance. Fourth is the mutual combination of the tangible battlefields with the intangible battlefields. IO with network and electronic [warfare] {*wangdian*} as primary mainly is carried out on the intangible battlefields, such as in network space and in the EM spectrum field {*dianci pinpu lingyu*}, and is greatly different in comparison to the force-strengths and firepower on the traditional tangible battlefields, with their "glint and flash of cold steel" {"刀光剑影" *"daoguang jianying"*} and "floating clouds of smoke" {"硝烟弥漫" *"xiaoyan miman"*}. The combination of the tangible battlefields with the intangible battlefields means the need to use "quiet" {*"jijing"*} or invisible CNW, EW, and PSYWAR, along with fierce firepower warfare and special operations {*tezhong zuozhan*}, mutually complemented, and adjusted-coordinated consistently to strike at the enemy, and protect oneself.

(4) Working hard to innovate IO fighting methods

In implementing and applying joint campaign IO guidance thought, innovating a set of effectual fighting methods is especially important. Laying stress on innovating fighting methods and excelling at innovating fighting methods not only are a superiority of our military, but also are traditions of our military. Innovating fighting methods within joint campaign IO requires having new trains of thought {*silu*} and new measures. First is the need to innovate in terms of the combination of tactics and technology. In the history of war in ancient and modern times, both in China and abroad, the most effective fighting methods without exception have been {无一不是 *wuyi bushi*} the products of the optimum combination {*zuijia jiehe*} of tactics and technology. In innovating fighting methods in terms of the combination of tactics and technology, what is most important is the need to have a deep understanding of and scientific attitude toward the performance and characteristics of information technology [IT] {*xinxi jishu*} and its equipment

{*zhuangbei*}, as well as of the important influence they have had on modern operations – and, on this basis, to boldly explore {*tansuo*} the methods used and the handling measures, and work hard to create new fighting methods complying with the requirements of IT and its equipment and adapting to our military's situation. Second is the need to innovate in terms of the combination of high technology and general technology. At present, although our military possesses several IO "assassin's mace" weapons and equipment, nonetheless much more in evidence is general-technology weapons and equipment. Hence, how to use low-tech to defeat high-tech {以低制高 *yidi zhigao*} and how to use indigenous methods to defeat foreign methods {以土制洋 *yitu zhiyang*} are the basic footholds {*lizudian*} for innovation of IO fighting methods. On one hand, [we] must conscientiously study effective measures for bringing into play the might of the "assassin's mace" weapons, **[end of page 56]** to fully bring into play the effectiveness of the limited high- and new-tech weapons and equipment. On the other hand, even more important is to find ways and means {想方设法 *xiangfang shefa*} to seek new avenues for bringing into play the might and employment of the large quantities of general-technology weapons and equipment we possess, so that they produce new combat power. At the same time, [we] also must concentrate our efforts {下功夫 *xia gongfu*} and write articles on the combination of "assassin's mace" weapons and general-technology weapons and equipment, so that the two superiorities are complementary {*youshi hubu*} and form a composite strength {*heli*}. Third is the need to innovate in terms of the combination of "soft" and "hard" means. During the Kosovo War and Iraq War, the practice {*zuofa*} of the US military – whereby it mutually combined "soft" means such as network attacks and electronic jamming with "hard" means such as precision strike {*jingque daji*}, and thus seized and maintained battlefield information dominance – is worth our drawing upon for reference. [We] must bring into play the respective strong points of the two means, for jointly defeating the enemy.

Section 2: Operational Principles…57

The basic principles of joint campaign IO are the basic criteria {*zhunze*} for embodying joint campaign IO laws and for guiding joint campaign IO activities. Under circumstances where the enemy is strong and we are weak {*diyou wolie*} in overall terms of IO weapons and equipment, upholding the IO principles which have our military's characteristics and are scientific will have extremely important significance for guiding our military's future joint campaign IO activities and for effectively bringing into play the maximum operational effectiveness.

I. Requirements for formulating IO principles…57

Within our military's future joint campaigns, IO will penetrate from start to finish of entire campaigns, and will have important influences on the campaigns. [We] must conscientiously study joint campaign IO laws under informationized war conditions, comprehensively analyze {*quanmian fenxi*} the strong and weak points of our future operational opponents in terms of IT[-based] weapons and informationized operations

theory, and combine these with our military's present IO capabilities and future joint campaign characteristics, to formulate joint campaign **[end of page 57]** IO basic principles having our military's characteristics, so as to enhance the directed [focused] quality and effectiveness of our military's future joint campaign IO activities guidance. When formulating the basic principles for joint campaign IO, [we] mainly should be based on the following several aspects:

(1) Implementing joint operations thought {*lianhe zuozhan sixiang*}

Joint gaining of victory {*lianhe zhisheng*} is a basic characteristic and law within modern war. In particular, several local wars which have occurred around the world since the 1990s even more fully have proven this point. Following on the development of IT, integrated {*yitihua*} information systems have provided even more advanced means for joint campaigns, and have enabled the land, sea, air, space, and EM multidimensional {*lu, hai, kong, tian, dian duowei*} operational strengths, via rapid and effective information linkup {*goutong*}, to achieve integrated-whole operational effectiveness {*zhengti zuozhan xiaoneng*}. Joint campaign IO activities too are like this. If [we] desire to achieve the goals of sabotaging the enemy's information and information systems and protecting friendly information capabilities, [we] must in a thorough and careful manner adjust-coordinate and apply the IO strengths of the three services (Army, Navy, and Air Force) and the Second Artillery Corps, as well as of other support units, and "hard" and "soft" IO means distributed over the 5-dimensional battlespace {*wuwei zhanchang kongjian*}, to form integrated-whole or local information superiority over the enemy, and – while ensuring the multiplication of friendly combat power – cause the demultiplication {倍减 *beijian*} of the enemy's integrated-whole combat power.

(2) Laying stress on seizing and maintaining local information dominance

The goal of joint campaign IO is to synthetically apply various IO strengths, via a series of IO activities, so as to seize and maintain battlefield local information dominance. Hence, within operations-research-based planning and organizing of joint campaign IO, [we] must from start to finish focus on this ultimate objective {*mubiao*}: seizing and maintaining battlefield local information dominance. In this way [we] can effectively adjust-coordinate and fully grasp the various types of relationships within joint campaign IO; achieve the mutual complementation of information offense and information defense; adjust-coordinate the application of soft kill and hard destruction means; and achieve mutual supplementation {相辅相成 *xiangfu xiangcheng*} among EM space, network space, and psychological space.

(3) Combining [the above] with the actual situation of our military's IO building

Our military's IO building got started fairly late. Although in recent years [we] have accelerated the development steps, **[end of page 58]** and in some fields have achieved prominent results, nonetheless from the overall viewpoint our military's IO strengths in qualitative and quantitative respects still show a fairly large gap compared to

the military powers. [Our] battlefield information reconnaissance {*xinxi zhencha*}, early warning, communication, IW {*xinxi duikang*}, and information defense capabilities overall still are relatively weak. We must have a clear-headed understanding {*renshi*} of this. However, war always has been a comprehensive trial of strength in strengths and wisdom {智慧 *zhihui*}, and on the basis of certain material strengths, the subjective dynamic quality {*zhuguan nengdongxing*} of war guidance has an extremely important role. Our military's future joint campaign IO also must uphold this guidance thought. On one hand, [we] must be grounded in our actual national conditions and military conditions, and be grounded in fighting battles with the equipment we have {有什么装备打什么仗 *you shenme zhuangbei da shenme zhang*}; and cannot simply and mechanically crack the hard nuts {*pengying*} with a powerful enemy. Instead, [we] must fully draw upon and develop IO theory having our military's characteristics, uphold "we'll let you fight your way, and we'll fight our way" {*"nida nide, woda wode"*}, and to the maximum extent bring into play the strong points of our IO strengths. On the other hand, [we] must lay the fullest stress on fully bringing into play the elite troops and efficient instruments {*jingbing liqi*} of our military's IO, and under circumstances of overall inferiority {*ruoshi*}, take care in the important phases and time segments to concentrate force-strengths and weapons, to form local superiority over the enemy, and achieve the IO effects of sabotaging the enemy nodes and paralyzing the enemy SoS.

(4) Aiming at {*miaozhun*} future operational opponents

The joint campaigns carried out by our military in the future will be counter-secessionist {*fanfenlie*}, counter-interventionist {*fanganyu*}, multi-service and arm joint campaigns conducted in order to maintain {*weihu*} national sovereignty and territorial integrity. The main operational opponent in recent years has shown fairly rapid development in the building of information strengths; organized and built professional IO units; accelerated development of IO equipment; numerous times conducted IO exercises with us as the imaginary enemy; and attained fairly strong operational capabilities in reconnaissance and early warning, EW, and network warfare [CNW] respects. The neighboring country on the southwest border, in order to realize the strategic goal {*zhanlue mudi*} of seeking hegemony {称霸 *chengba*} in Southern Asia, has constantly strengthened its military real power {*junshi shili*}. In recent years, it has especially attached importance to bringing into play its native IT and talent superiorities, strengthened military technical cooperation with the West, and attached importance to self-development {自研 *ziyan*} of IO weapons; and its integrated-whole IO capability already has attained a substantial level. In addition, the informationized levels {*xinxihua shuiping*} of the world's military powers all along have been in a leading position, and in IO respects already **[end of page 59]** have attained full-dimensional reconnaissance and surveillance [R&S] {全维侦监 *quanwei zhenjian*} and accurate real-time reconnaissance and early warning capabilities; high-integration-level {*jichengdu gao*}, rapid and high-efficiency information transmission and processing {*xinxi chuandi he chuli*} capability; information offense capability having both soft and hard [means] {软硬兼备 *ruanying jianbei*} and a combination of points and areas {*dianmian jiehe*}; and peacetime-wartime integrated {*pingzhan yiti*}, jam-resistant and destruction-resistant {*kangrao, kanghui*}

information defense capability. [Moreover, the military powers'] IW {*xinxizhan*} and precision warfare {*jingquezhan*} already have gradually taken over the leading position within their future operational activities, and within several recent local wars have attained full development. Hence, on the background of a powerful enemy's possible intervention, future joint campaign IO will be faced with severe challenges. This then requires that we pay close attention to developing advanced IO strengths, conscientiously study our future operational opponents, draw upon their experience and strong points, analyze their inadequacies and weak points, and formulate and adopt effective countermeasures {*duice*}. Only by knowing the enemy and yourself {*zhiji zhibi*} can you fight a hundred battles with no danger of defeat {*baizhan budai*}, and within future military struggle be in an invincible [position] {*liyu bubai*}.

II. Content of the basic principles of IO…60

The content of the basic principles of joint campaign IO is as follows: full preparations and thorough operations-research-based planning; unified command {*tongyi zhihui*} and close coordination {*miqie xietong*}; concentration of the elite {*jingrui*}, to attack enemy vital sites; concealment and surprise {*yinbi turan*}, and [seizing] the first opportunity to subdue the enemy; and rigorous protection, to ensure security.

(1) Full preparations and thorough operations-research-based planning

Full preparations and thorough operations-research-based planning signify, in peacetime and in the imminent battle preparation phase {*linzhan zhunbei jieduan*}, thoroughly and ably performing all items of the preparatory work for IO, including theoretical research, exploitation {*kaifa*} of technology, cultivation (training) of talent {*rencai peiyang*}, battlefield and unit building, formulation of plans {*jihua*}, and readiness training {*zhanbei xunlian*}. In wartime, based on the joint campaign's actual situation, the commander's {*zhihuiyuan*} operational intent {*zuozhan yitu*}, the IO missions, and the task organization {*biancheng*} situation of the IO strengths, [command personnel] carry out integrated-whole operations-research-based planning and working out an approach in planning {*zhengti chouhua yu mouhua*} for all types of IO strengths and IO activities, take all things into consideration {通盘考虑 *tongpan kaolyu*}, and do unified operations-research-based planning of arrangements {*tongchou anpai*}, to see that IO becomes an organic component of the joint campaign. Under circumstances where our military's IO weapons and equipment will be in an inferior position compared to a powerful enemy, via in-advance {*yuxian*} full preparations and thorough operations-research-based planning, [we] can reduce the gap with the opponent, as rapidly as possible change the inferior position into a superior position, and thus lay a solid foundation for defeating the enemy. These are prerequisites {*qianti tiaojian*} for ensuring that joint campaign IO is smoothly **[end of page 60]** implemented.

In implementing the principle of full preparations and thorough operations-research-based planning, first is that [command personnel] should fully exploit favorable conditions for peacetime IO preparations, and strengthen {*jiaqiang*} and perfect the

building of IO battlefields and strengths in the main direction and key point areas {*zhongdian diqu*}. Second is synthetically applying multiple information reconnaissance means to understand and grasp the enemy IO-related situation. Third is, based on the joint campaign operational courses of action [COAs] {*zuozhan fang'an*}, thoroughly formulating IO plans; based on the operational missions and the battlefield environment, organizing imminent battle preparations in a manner having a directed [focused] quality; doing a good job of IO preparations and materiel preparations {*wuzi zhunbei*}; in a deep and careful manner, ably performing the thought and political work of the IO units; and carrying out the mobilization {*dongyuan*} and organizational work for the participation {*canzhan*} of the local IO strengths. Fourth is, after receiving the operational missions, swiftly, comprehensively, and accurately grasping the IO-related battlefield situation, doing thorough operations-research-based planning for IO activities, with the key points on clarifying the IO goals, main targets/objectives, basic fighting methods, and operational disposition {*zuozhan bushu*}; carrying out scientific organization and allocation {*bianpei*} and combination of the IO strengths, and forming a SoS of IO strengths, deployed properly, mutually linked up {*xianghu xianjie*}, and distributed rationally {*buju heli*}; correctly formulating the IO objectives, time opportunities, spatial domain {*kongyu*}, and frequency domain {*pinyu*}, and thoroughly formulating the IO plans; and thoroughly organizing the coordination and support, to boost the IO effectiveness.

(2) Unified command and close coordination

Unified command and close coordination signify applying advanced command means {*zhihui shouduan*} to put into effect integrated command {*yitihuade zhihui*} of all participating services and arms and local IO strengths; to strengthen the coordination of the main battlefield and main direction, as well as of the main-battle large formations {*zhuzhan juntuan*} and IO strengths; and to ensure [the conduct of] activities under the unified campaign intent {*tongyide zhanyi yitu*} and objectives. The joint campaign IO strength composition {*liliang goucheng*} is complex, the operational methods and means are diversified, and the fields involved are expansive and tightly combined with other operational activities. Only by putting into effect highly centralized and unified command {*jizhong tongyide zhihui*} and close coordination can [command personnel] ensure that the various strengths of joint campaign IO from start to finish center on the overall situation of the campaign [and] are adjusted-coordinated consistently in their activities.

In implementing the principle of unified command and close coordination, first is the need to use the IO **[end of page 61]** guidance thought to unify the IO activities of all services and arms, and see that all units' IO activities tightly center on the unfolding of the IO goals. Second, according to the requirements for authoritativeness {*quanwei*}, eliteness {*jinggan*}, agility {*lingbian*}, and high efficiency {*gaoxiao*}, is establishing integrated {*yitihua*} joint campaign IO command institutions {*zhihui jigou*}, clarifying the command relationships {*zhihui guanxi*} and command authority limits {*zhihui quanxian*}, unifying the organization and use of the IO strengths, doing unified operations-research-based planning {*tongyi chouhua*} for the activities of the subordinate

IO units, and fully bringing into play the integrated-whole effectiveness of the various IO strengths and operational activities; relying on the campaign command information systems to perfect the IO command network, and to ensure the smoothness and high efficiency of IO command; and, based on the battlefield situation, flexibly {*linghuo*} adopting the corresponding command modes {*zhihui fangshi*}. Third, based on the characteristics of the various IO strengths, is properly {*qiadang*} entrusting the missions. Based on the joint campaign IO resolution {*xinxi zuozhan juexin*}, the IO plans, and the higher-level coordination instructions {*shangji xietong zhishi*}, [this involves] thoroughly formulating the IO coordination plan; clarifying the coordination relationships, methods, and requirements; particularly organizing electronic jamming and network attack activities; ably adjusting-coordinating the attack directions, targets, and time opportunities; and avoiding causing jamming of friendly information and information systems. Fourth, with planned coordination {*jihua xietong*} as primary, and based on developing changes in the IO posture {*xinxi zuozhan taishi*}, is timely organizing ad hoc coordination {*linji xietong*}, strengthening coordination support, and formulating recovery COAs when coordination suffers sabotage, to maintain uninterrupted {*bujianduan*} coordination.

(3) Concentrating the elite, to attack the enemy vital sites

Concentrating strengths to attack the enemy vital sites signifies, within a certain time, accurately selecting the enemy information system's weak links and critical nodes, concentrating use of elite information offensive strengths, and implementing continuous attacks {*lianxu gongji*}, to achieve the goals of effectively sabotaging the enemy information systems and reducing {减煞 *jiansha*} the enemy's operational capability.

In implementing the principle of concentrating the elite to attack the enemy vital sites, first, based on joint campaign IO requirements, combined with the situation of the IO strengths, is assembling {*diaoji*} the elite strengths for strategic and campaign {*zhanlue zhanyi*} IO, and weaving them into the joint campaign large formations, to enhance IO capability. Second is concentrating the IO elite strengths in the main operational direction, main battlefield, main phases, and critical time segments, to form local superiority. Third is meticulously selecting the enemy's important networks, **[end of page 62]** critical nodes, and weak links; forming a powerful information offense posture; flexibly applying soft and hard strike means and methods; and implementing key point strikes, to paralyze, sabotage, and [/or] weaken the enemy information system functions {*gongneng*}. Fourth, on the basis of an all-around grasp and understanding of the enemy information system's weak links and critical nodes, is comprehensively considering the feasibility and effectiveness of realizing the objectives, and determining the key point strike targets. Fifth is the need to timely track and understand the execution situation for the information offense activities, evaluate-appraise {*pinggu*} the strike and sabotage effects, achieve "real-time control {*shishi zhangkong*}," and watch the situation to effect adjustments {*tiaozheng*} to the offensive strengths and intensity.

(4) Concealment and surprise and [seizing] the first opportunity to subdue the enemy

Concealment and surprise and [seizing] the first opportunity to subdue the enemy signify synthetically applying various methods and means to conceal the IO intent and activities; deceive and confuse {*qipian mihuo*} the enemy; and strive at times, places, and targets unimaginable to the enemy to concentrate information offense strengths, execute surprise attacks, and restrict the enemy in a passive position.

In implementing the principle of concealment and surprise and [seizing] the first opportunity to subdue the enemy, first is fully and ably carrying out the IO preparations, formulating multiple contingency preliminary COAs {*yingji yu'an*}, and ensuring at any time the conduct of IO activities. Second, based on the battlefield situation, is selecting and creating opportunities for combat, and striving to launch an information attack before the enemy and to maintain the battlefield initiative. Third is adopting strict secrecy {*baomi*} measures to conceal the IO intent. [This means] strengthening strict management of information systems and IO equipment, conducting secrecy education for personnel involved with secrets {*shemi renyuan*} [i.e., cleared personnel], and guarding against the occurrence of cases of careless and other leaks of secrets {*shi, xiemi shijian*}. Fourth is attaching importance to using information deception {*xinxi qipian*} means; concealing the true and displaying the false {*yinzhen shijia*} with respect to the friendly operational intent, disposition, and activities; and [thus] achieving the goals of confusing and moving {*diaodong*} the enemy and causing the enemy errors in judgment and decision-making {*panduan, juece*}. Fifth is grasping the battlefield situation and the changes in the IO posture, and from start to finish maintaining the advantage of the first opportunity.

(5) Rigorous protection, to ensure security

Rigorous protection to ensure security signifies, based on the characteristics of enemy information offense, adopting protective measures in a manner having a directed [focused] quality, and to the maximum extent reducing the enemy's degree of damage {*huishang chengdu*} to our information systems, to ensure our military's operational INFOSEC and the stable operation {*yunxing*} of our information systems. **[end of page 63]** Within future wars, a powerful enemy will rely on information superiority, and by various means conduct full-dimensional {*quanfangwei*} electronic reconnaissance and high-intensity electronic attacks against our command information system. Only by adopting rigorous information protection and eliminating the direct threats to the composition of our information system can [we] effectively protect the security of battlefield information systems.

In implementing the principle of rigorous protection to ensure security, first is that the joint campaign commander [JCC] {*lianhe zhanyi zhihuiyuan*} and his command organ {*zhihui jiguan*} should set out from the overall situation of the campaign, unify the organization and operations-research-based planning of information protection activities,

lay stress on the protection key points, and strengthen the protection for important targets such as the vital site positions and critical nodes within the command information system, to ensure the security of battlefield information and information systems. Second, based on the characteristics of the enemy information offense, combined with the battlefield reality, is adoption of information protection measures in an all-around, key point manner, having a directed [focused] quality, to ensure that our side effectively acquires, transmits, processes, and exploits operational information. [This means] boosting the information system's counter-reconnaissance {*fanzhencha*}, counter-jamming {*fanganrao*}, counter-stealth {*fanyinshen*}, and counter-destruction {*fancuihui*} capabilities. Third is synthetically applying multiple information offense means to assist-support and complement {*zhiyuan peihe*} the protection of important targets. Fourth is implementing an INFOSEC secrecy system {*xinxi anquan baomi zhidu*}, strictly adhering to the various specifications {*guiding*}, and guarding against the leak of important IO secrets and EM information leakage {*dianci xinxi xielou*}. Fifth is strengthening self-protection {*zishen fanghu*} for the IO professional strengths, to boost battlefield survivability.

III. Several issues which should be given attention when implementing and applying the basic principles of IO…64

The basic principles of joint campaign IO have reflected the basic laws of joint campaign IO, and possess a fairly strong directed [focused] quality and guidance quality. However, within future joint campaign activities, due to the differences in campaign patterns {*zhanyi yangshi*}, the differences in the battlefield environment, and the differences in the objects of operations {*zuozhan duixiang*}, and in particular following on the constant development of IT, both the modes and the methods of IO may undergo fairly great changes. Hence, within joint campaign IO activities, [the JCC and his command organ] must, based on the specific {*juti*} situation, overall grasp and flexibly apply the above principles, and must not apply them mechanically or indiscriminately {生搬硬套 *shengban yingtao*}. At the same time, they also must, via large amounts of training or real combat testing {*shizhan jianyan*}, constantly summarize and develop new operational principles. **[end of page 64]**

(1) Overall grasp

Joint campaign IO is an operational SoS which involves a broad scope and complex relationships. Within the operational process, [the JCC and command organ] not only must adjust-coordinate the relationships among the various IO forms {形式 *xingshi*}, including EW, network warfare [CNW], and PSYWAR, but also must keep an eye on the relationship between IO and the joint campaign's other operational activities; they not only must actively implement information offense, but also must attach high importance to their own information protection; and they not only must fully grasp the attack and defense activities {*gongfang xingdong*} for soft-kill information weapons, but also must pay attention to information attack and defense activities for hard-kill weapons. The JCC and his command institution, when organizing operations-research-based

planning of IO, should from the overall viewpoint grasp the key points in IO strength employment and in information offense and defense, in the adjusted-coordinated application of soft-kill means and hard-kill means, and in stratagem guidance {*moulue zhidao*} for information weapons technology and IO; focus on the overall situation; take all things into consideration; make overall use of mathematical and scientific methods {*zongti yunchou*}; and guard against attending to one thing while losing sight of the other.

(2) Flexible application

The basic principles of joint campaign IO are the basic criteria guiding the joint campaign IO activities, and have a universal quality {*pubianxiang*}. Due to the differences in joint campaign patterns, the differences in the objects of operations, and the differences in the operational environment, joint campaign IO under different conditions thus will have individual different characteristics. This then requires that we organically combine the basic, universal-quality IO principles together with the specific situation, and, based on the different joint campaign IO situations, flexibly apply these guidance principles well. In addition, [we] also must combine them with the specific situation of the campaign and thus carry out detailing {*xihua*} of these basic principles, to enhance their operability {*caozuoxing*}, so that every IO activity can obtain scientific and effective guidance. In the different phases carried out in a campaign, the key points of IO will differ, and will require timely adjustment of the guiding principles.

(3) Innovating development

Joint campaign IO is a new topic {*keti*} facing our military within the process of realizing the dual historic mission of mechanization and informatization. In recent years, although all levels of our military's senior officers {*shouzhang*}, **[end of page 65]** organs, and units all have attached unusual importance to study of [research on] this topic, nonetheless, due to the restrictions on IT levels and the lack of corresponding experience in practice, studies of the laws and characteristics of joint campaign IO still are insufficiently deep and all-around. These inadequacies are reflected in studies of the IO principles, and it should be said that there are still a good many fields not understood or not understood clearly. The above five basic principles still are only an initial research achievement, and still await further testing and perfection within future training and operational practice. From the viewpoints of the development of IT within the world scope and of the trend of its application in the military field, the progress {*jincheng*} of military informatization is still far from being completed, while IT is still being constantly developed and perfected, and, in mutual adaptation to this, new IO patterns also are constantly emerging. Hence, studies of the basic principles of joint campaign IO likewise may constantly be adjusted following on the development of the times and of technology. [We] must keep our eyes on development, and keenly acquire insight into and forecast {*yuce*} the influence of the developing changes in the information field on information operations, uphold liberation thought, and constantly innovate and develop information operations basic principles adapted to our military's actual situation. Only in

this manner can [we] adapt to the development of the times, seize the initiative within the worldwide tide of informationized military revolution [i.e., Revolution in Military Affairs (RMA)], and within future military struggle be in an invincible position {*liyu bubai zhidi*}. **[end of page 66; end of chapter]**

This page intentionally left blank.

Chapter 4
Joint Campaign Information Operations Strengths {*liliang*}…67

Joint campaign information operations (IO) strengths signify the general term for the various types of strengths participating in joint campaign IO, under a unified intention and guidance {*tongyi qitu he zhidao*}. They are an important component {*zucheng bufen*} of joint campaign operational strengths.

Section 1: Characteristics {*tedian*} of Joint Campaign IO Strengths…67

The practice of several recent local wars has proven that joint campaign operations – no matter whether in terms of external features {*tezheng*} or essential connotations {本质内涵 *benzhi neihan*} – always have undergone profound changes. Most prominent is that the information essential factors {*xinxi yaosu*} already have become the basic essential factors in armed forces combat power {*jundui zhandouli*}, and joint campaign IO strengths also have already become important support {*zhicheng*} for the joint campaign strengths.

I. Infiltration {*shentou*} into many fields {*lingyu*}, involvement of many levels {*cengci*}, and possession of a high degree of wide-zone quality {*guangyuxing*}…67

Following on the development of information technology [IT] {*xinxi jishu*} and its wide application in the military, the battlefield environment is undergoing hitherto unknown changes, and the operations field no longer is limited to the traditional battlespace {*zhanchang kongjian*}. The trends toward weapons and equipment informatization {*wuqi zhuangbei xinxihua*} and information equipment weaponization {*xinxi zhuangbei wuqihua*}, and their interdynamic development {*hudong fazhan*}, mutual fusion {*huxiang ronghe*}, and mutual infiltration {*huxiang shentou*} have caused the extension {*waiyan*} and connotations of joint campaign IO strengths to attain maximum expansion. Joint campaign IO strengths already have infiltrated into the midst of all operational activities {*zuozhan xingdong*}. First is their infiltration into various fields, including the military, political, science and technology [S&T] {*keji*}, **[end of page 67]** economic, and security {*anquan*} [fields]. IO has a very strong political quality and strategic quality {*zhanluexing*}; the military activity {*huodong*} of the engaging sides {*jiaozhan shuangfang*} can upward connect {*shanglian*} to heads of state and state organs {*guojia shounao jiguan*}, and reach down to the common masses. For example, intrusions {*qinru*}, attacks {*gongji*}, and sabotage {*pohuai*} against important information networks not only can come from military function institutions {*junshi zhineng jigou*}, but also can come from nongovernmental computer hackers {*minjian heike*}. Second is their infiltration into all levels: strategic, campaign, and tactical. Information activity has broken through the traditional battlefield demarcation lines; the operational level is not clearly demarcated {*jieding*}, and there even could arise a tendency [for the levels] to coincide {*chonghe*}. For the side which holds information superiority {*xinxi youshi*}, the battlefield's unidirectional transparency {*danxiang*

toumingdu} will be high. That side will have the capability to simultaneously execute strikes against the battlefield's full depth {*quan zongshen*}, including strategic, campaign, and tactical objectives {*mubiao*}; beyond-time-and-space {*chaoshikong*} command and control [C2] {*zhihui kongzhi*} capability; and long-range precision strike {*yuancheng jingque daji*} capability. These enable tactical strikes to directly achieve campaign and even war goals {*zhanzheng mudi*}, and command networks with IT as their support {*zhicheng*} enable strategic command {*zhanlue zhihui*} at any time to intervene at the tactical level. In future operations, the characteristics of strategic-level decision-making {*zhanlueji juece*}, campaign-level command, and tactical-level activities will be even more prominent. Third is their infiltration into all systems {*xitong*} of weapons and equipment. IO strengths have a very strong dependent quality {*yifuxing*} and fused quality {*ronghexing*}; many cannot separately bring into play a role {*zuoyong*} independent of the other operational strengths, but must be mutually combined with the other strengths, and interact {*xianghu zuoyong*} with them, to jointly produce operational effectiveness {*zuozhan xiaoneng*}. At the same time, weapons and equipment systems also are becoming more informationized day by day.

II. Compositional essential factors are complex, and momentum disposition is decentralized {*bushi fensan*}; possession of a distinct multidimensional quality {*duoyuanxing*}…68

Joint campaign IO strengths in terms of composition possess a multidimensional quality. They not only include professional {*zhuanye*} IO strengths, but also include nonprofessional IO strengths; they not only include sea and land IO strengths, but also include air and outer space {*kongzhong, taikong*} IO strengths; they not only include conventional {*changgui*} IO strengths, but also include unconventional IO strengths; and they not only include material {*wuzhi*} IO strengths to strike at and sabotage enemy weapons and equipment, but also include IO strengths to attack the enemy's consciousness and thought {*yishi, sixiang*}. The IO strength distribution is extremely wide-ranging. First is the dispersal of professional IO strengths over the entire battlespace. Professional IO strengths involved in many aspects, such as electronic warfare [EW] {*dianzizhan*}, network warfare {*wangluozhan*}, and psychological warfare [PSYWAR] {*xinlizhan*}, are interwoven together with other operational strengths, **[end of page 68]** and will be jointly active with them over the entire battlefield of the future. Second is the wide participation of the nonprofessional IO strengths. Against those targets where application of means such as high-tech intelligence warfare {*qingbaozhan*}, network warfare, and EW has difficulty proving effective, [we] can apply the method of a mutual combination of nonprofessional IO strengths with means such as traditional reconnaissance {*zhencha*}, special operations {*tezhong zuozhan*}, firepower attack, and activities deception {*xingdong qipian*}, and can [thus] completely destroy or sabotage the enemy information systems. Third is the joint integration {*lianhe yiti*} of peacetime and wartime military-civilian {*pingzhanshi junmin*} IO strengths. IO is boundless and borderless {*wujiang wujie*}, intangible and formless {*wuxing wuxiang*}, and present at all times {*wushi buzai*}; and the peacetime-wartime demarcation line tends to blur, so that peacetime and wartime information strengths are present all along.

III. Task organization {*biancheng*} and employment integration requirements {*shiyong yitihua yaoqiu*} are stringent; possession of a complex systematic quality {*xitongxing*}…69

Under the effect of system integration {*xitong jicheng*}, the various essential factors of joint campaign IO strengths constitute an organic integrated whole {*youji zhengti*}, to conduct system confrontation {*xitong duikang*} and system-of-systems [SoS] warfare {*tixi duikang*}. First of all, the integrity {*wanzhengxing*} of the information flow path requires that the four links {*huanjie*}, information acquisition, processing, transmission, and exploitation {*xinxi huoqu, chuli, chuanshu, liyong*}, must constitute an organic whole {*yiti*}, and cannot be broken apart {*fen'ge*}. The various parts are both mutually independent {*xianghu duli*} and mutually conditional {*huwei tiaojian*}, mutually correlated {*xianghu guanlian*} and mutually restrictive {*xianghu zhiyue*}. Next, information systems and main battle weapons and equipment are joined into an organic whole {*yiti lianjie*}, to bring into play their might {*weili*}. Operations no longer are single confrontations of weapons and equipment, but rather are system confrontations composed of various strengths, ground, sea, air, and outer space, under the joining of information systems. Third, the IO strengths [form a] system synthesis {*xitong hecheng*}, with interconnection, intercommunication, and interoperability {*hulian, hutong, hucaozuo*}; the entire information battlefield is joined into an organic whole. This causes operational activities to be adjusted-coordinated {*xietiao*} consistently, and joins all spaces, land, sea, air, space, and electromagnetic [EM] {*lu, hai, kong, tian, dian*}, into one enormous full-dimensional IO network {*quanwei xinxi zuozhan wangluo*}.

Section 2: Classification {*fenlei*} and Task Organization of Joint Campaign IO Strengths…69

The joint campaign IO strengths are an important material basis for carrying out joint campaign IO. Correctly recognizing the types {*leixing*} of joint campaign IO strengths and their composition **[end of page 69]** has important significance for achieving the joint campaign IO goals.

I. Classification of joint campaign IO strengths…70

The classification of joint campaign IO strengths can be differentiated from different standpoints. From the standpoint of service and arm structure {*junbingzhong jiegou*}, they can be differentiated into Army, Navy, Air Force, and Second Artillery Corps IO strengths for joint campaign IO, and armed police unit {*wuzhuang jingcha budui*} and local {*difang*} IO strengths. From the standpoint of mission nature and functional structure {*zhineng jiegou*}, they can be differentiated into IO command strengths, IO attack and defense strengths {*gongfang liliang*}, and IO support strengths

{*baozhang liliang*}.[8] From the standpoint of damage form {*huishang xingshi*}, they can be differentiated into IO "soft strike" {*"ruan daji"*} and "hard destruction" {*"ying cuihui"*} strengths. From the standpoint of professional type, they can be differentiated into professional IO strengths and nonprofessional IO strengths. The basic classification of joint campaign IO strengths mainly includes the following two types:

(1) "Soft strike" and "hard destruction" IO strengths

"Soft strike" strengths mainly include four types: the first is electronic jamming {*dianzi ganrao*} strengths, such as radar jamming {*leida ganrao*}, communication jamming {*tongxin ganrao*}, electro-optical [E-O] jamming {*guangdian ganrao*}, and hydroacoustic jamming {*shuisheng ganrao*}. The second type is computer network attack {*jisuanji wangluo gongji*} strengths, such as for computer virus attack {*jisuanji bingdu gongji*} and computer hacker infiltration {*heike shentou*}. The third type is psychological attack {*xinli gongji*} strengths, such as for psychological attacks carried out by methods like TV, radio, printed matter, and virtual reality [VR] {*xuni xianshi*} technology. The fourth type is intelligence warfare strengths, such as for deliberately transmitting false intelligence {*weijia qingbao*} to enemy intelligence systems and for acquiring intelligence from the enemy.

The "hard destruction" strengths mainly include the following: first are the precision and conventional fire strike strengths; second are anti-radiation attack {*fanfushe gongji*} strengths; third are special information warfare [IW] weapons {*teshu xinxizhan wuqi*} (laser {*jiguang*}, high-power microwave [HPM] {*gaoneng weibo*}, particle beam {*lizi shu*}, EM pulse {*dianci maichong*}, and carbon fiber weapons {*tan xianweisi wuqi*}); and fourth are non-lethal [quality] weapons {*feizhimingxing wuqi*}.

(2) Professional and nonprofessional IO strengths

1. Professional IO strengths

Professional IO strengths signify the strengths specially used for conducting IO. **[end of page 70]** They are the mainstays of joint campaign IO, and have a task organization of IO professional strengths sent by higher levels as reinforcements {*jiaqiang*}, plus those within the root-level organizational system {*benji jianzhi*}. They usually include the following: joint campaign directly subordinate IO strengths, with a task organization of IO units (elements) {*bu (fen) dui*} directly commanded by the joint campaign command institution {*zhihui jigou*}; Army IO strengths, with a task organization of the Army's various group army {*jituanjun*} IO units (elements); Navy IO

[8] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

strengths, with a task organization of the Navy's various IO units (elements); Air Force IO strengths, with a task organization of the Air Force's various IO units (elements); and Second Artillery Corps IO strengths, with a task organization of Second Artillery Corps IO units (elements).

2. Nonprofessional IO strengths

The nonprofessional IO strengths, relative to the professional IO strengths, mainly indicate other operational strengths which are outside the IO task organization, and used for assisting-supporting {*zhiyuan*} and complementing {*peihe*} the professional IO strengths and for fulfilling IO missions. The nonprofessional IO strengths, such as the fire strike strengths and the local support-the-front strengths {*difang zhiqian liliang*} for assisting support to IO, are an important component of the joint campaign IO strengths. Under the current circumstances where our military's IO professional strengths are fairly limited, we should fully bring into play the role of nonprofessional IO strengths, to enhance IO capability.

Special operations sabotage-raid {*poxi*} information system strengths signify, within implementation of IO, operational strengths which apply the special operations forces {*tezhong zuozhan budui*} (groupings {*qun*}) of all campaign-participating services and arms to sabotage the enemy information systems. They mainly include the following: special reconnaissance {*tezhong zhencha*} and strike units (elements), as well as units (elements) which can execute special IO missions.

The local IO strengths usually are composed of the IO strengths of the posts and telecom {*youdian*}, telecommunications {*dianxin*}, mobile communication {*yidong tongxin*}, electric power, railway and traffic {*tielu yu jiaotong*}, aviation, finance, and propaganda departments, which assist-support or complement the campaign operations.

II. Task organization of joint campaign IO strengths…71

Joint campaign IO strengths are an important component of the joint campaign strengths. **[end of page 71]** The scale of the joint campaign IO strength task organization must conform to the needs and requirements {*xuyao*} of the joint campaign missions, scale, and pattern {*zhanyi renwu, guimo, yangshi*}. The operational essential factors within the IO strength task organization must be complete {*qiquan*}, and must be mutually adapted to the mission undertaken {*danfu*}; they must increase the allocated proportion {*bianpei bili*} of advanced IO equipment, to boost IO capability; they must be convenient for command, adjusting-coordination, and support; and they must be beneficial to increasing to the maximum extent the adaptability {*shiying nengli*} to complex EM environments and to terrain, meteorological, hydrological, and other special battlefield environments. They usually have a task organization of the joint campaign's directly subordinate IO strengths, the IO strengths subordinate to the various services and arms, armed police units {*wujing budui*}, and requisitioned/commandeered {*zhengyong*} local IO strengths.

(1) Joint campaign directly subordinate IO strengths

These mainly have a task organization of reinforcing IO strengths sent by General Headquarters [HQ] {*zongbu*}, the attached {*peishu*} IO strengths transferred {*choudiao*} from the related military area commands [MACs] {*junqu*} and services and arms, and the requisitioned/commandeered local IO strengths. They usually include the following: EW {*dianzi duikang*} and special IW weapons, network warfare units (elements), and PSYWAR units (elements).

(2) Army IO strengths

These mainly have a task organization of IO units attached by higher levels and of IO units directly subordinate to the Army campaign large formation {*zhanyi juntuan*}. They mainly include the following: EW and computer network protection {*jisuanji wangluo fanghu*} units (elements) and intelligence warfare units (elements).

(3) Navy IO strengths

These mainly have a task organization of IO strengths attached by higher levels and of those directly subordinate to the naval campaign large formation. They mainly include the following: EW and computer network protection units (elements) and intelligence warfare units (elements).

(4) Air Force IO strengths

These mainly have a task organization of IO strengths attached by higher levels and of those directly subordinate to the Air Force campaign large formation. They usually include the following: EW, anti-radiation weapon attack, and computer network protection units (elements), and intelligence warfare units (elements). **[end of page 72]**

(5) Second Artillery Corps IO strengths

These mainly have a task organization of the IO strengths attached by higher levels and of those directly subordinate to the Second Artillery Corps campaign large formation. They usually include the following: EW, anti-radiation weapon attack, and computer network protection units (elements), and intelligence warfare units (elements).

(6) Armed police unit IO strengths

These mainly have a task organization of the IO strengths attached by higher levels and of those directly subordinate to the armed police units.

(7) Local IO strengths

These usually have a task organization of the IO strengths of the posts and telecom, telecommunications, mobile communication, electric power, railway and traffic, aviation, finance, and propaganda departments, which assist-support and complement the campaign [operations].

Section 3: Missions of the Joint Campaign IO Strengths…73

The basic missions of joint campaign IO are as follows: "to protect the security of friendly {*wofang*} campaign information and information systems, and the normal bringing into play of information system effectiveness; to harass {*raoluan*} and sabotage the enemy information systems; and to weaken their capability for acquiring, processing, transmitting, and using information." The IO strengths subordinate to all services and arms must, based on the missions of the root service and arm, fulfill IO assisting support missions.

I. Missions of the joint campaign's directly subordinate IO strengths…73

The IO strengths directly subordinate to the joint campaign large formation are the main strengths for seizing joint campaign local information dominance {*jubu zhixinxiquan*}. Their main missions are as follows: to organize and conduct IO reconnaissance {*xinxi zuozhan zhencha*}, mainly to ascertain the composition and application characteristics of the enemy's strategic and campaign information systems, plus the enemy IO strengths' task organization, disposition {*bushu*}, and activities intention {*xingdong qitu*}; under complementation by the campaign IO strengths of all services and arms, to execute electronic attacks and network attacks against the enemy's important strategic and campaign information and information systems; **[end of page 73]** to organize and execute psychological attacks, to weaken the enemy's popular support {*minxin*} and morale; to organize electronic camouflage and deception {*dianzi weizhuang, qipian*}, and coordinate {*xietong*} with other operational strengths in conducting campaign information defense {*xinxi fangyu*}; to assist-support the IO activities of all services and arms and the other operational activities of the joint campaign large formation; and together with the IO strengths of all services and arms, as well as related operational strengths, to jointly seize campaign local information dominance.

II. Missions of the Army IO strengths…74

The main missions of the Army IO strengths are as follows: to conduct campaign IO reconnaissance, mainly to ascertain the enemy system composition and application characteristics correlated to Army operations, plus the enemy IO strengths' task organization, disposition, and activities intention; to conduct information offense {*xinxi jingong*}, via key point jamming {*zhongdian ganrao*} and sabotage of enemy information systems constituting a threat to our Army operations; to organize electronic camouflage

and [electronic] diversion/demonstration {*dianzi weizhuang, yangdong*}, to carry out information deception {*xinxi qipian*} against the enemy; via active offensive activities {*jiji de jingong xingdong*}, to coordinate with the Army's other operational strengths in conducting information defense; to complement the IO activities of the campaign large formations of other services and arms, and assist-support the Army campaign large formation's other operational activities; to carry out special IO behind enemy lines {*dihou tezhong xinxi zuozhan*}; and to coordinate with the joint campaign large formation's directly subordinate IO strengths and the IO strengths of the campaign large formations of other services and arms, in jointly seizing campaign local information dominance.

III. Missions of the Navy IO strengths…74

The main missions of the Navy IO strengths are as follows: to conduct campaign IO reconnaissance, by synthetically applying {*zonghe yunyong*} sea, air, and shore-based IO reconnaissance platforms, mainly to ascertain the enemy information system composition and application characteristics related to naval operations {*haishang zuozhan*}, plus the task organization, disposition, and activities intention of the enemy naval IO strengths; to conduct information offense, by jamming and sabotaging the enemy's information and information systems which influence our Navy's operations; to organize electronic camouflage and [electronic] diversion/demonstration, to conduct information deception against the enemy; via active offensive activities, to coordinate with the Navy's other operational strengths in conducting information defense; to complement the IO activities of the campaign large formations of other services and arms, and assist-support the naval campaign large formation's other operational activities; and to coordinate with the joint **[end of page 74]** campaign large formation's directly subordinate IO strengths and the IO strengths of other services and arms, in jointly seizing campaign local information dominance.

IV. Missions of the Air Force IO strengths…75

The main missions of the Air Force IO strengths are as follows: to conduct campaign IO reconnaissance, mainly to ascertain the enemy information system composition and application characteristics correlated to Air Force operations, plus the task organization, disposition, and activities intention of the enemy IO strengths; to conduct information offense, by jamming and sabotaging enemy information and information systems which influence our Air Force operations; to assist-support the Air Force campaign large formation's other operational activities; to organize electronic camouflage and [electronic] diversion/demonstration, to conduct information deception against the enemy; via active offensive activities, to coordinate with the Air Force's other operational strengths in conducting information defense; to complement the IO activities of the campaign large formations of other services and arms, and assist-support the Air Force campaign large formation's other operational activities; and to coordinate with the joint campaign large formation's directly subordinate IO strengths and the IO strengths of the other services and arms, in jointly seizing campaign local information dominance.

V. Missions of the Second Artillery Corps IO strengths…75

The main missions of the Second Artillery Corps IO strengths are as follows: to conduct campaign IO reconnaissance, mainly to ascertain the enemy information system composition and application characteristics correlated to Second Artillery Corps operations, plus the task organization, disposition, and activities intention of the enemy IO strengths; to conduct information offense, by jamming and sabotaging enemy information and information systems which influence our Second Artillery Corps operations, and assist-support the Second Artillery Corps campaign large formation's other operational activities; to organize electronic camouflage and electronic diversion/demonstration, to conduct information deception against the enemy; via active offensive activities, to coordinate with the Second Artillery Corps' other operational strengths in conducting information defense; to complement the IO activities of the campaign large formations of other services and arms, and assist-support the Second Artillery Corps campaign large formation's other operational activities; and to coordinate with the joint campaign large formation's directly subordinate IO strengths and the IO strengths of the other services and arms, in jointly seizing campaign local information dominance. **[end of page 75]**

VI. Missions of the armed police units' IO strengths…76

The main missions of the armed police units' IO strengths are as follows: to grasp the in-theater {*zhanqu nei*} social situation and public feelings related to IO, and in particular the social outbreak situations {*tufa shijian qingkuang*} which influence campaign IO activities, so as to provide the correlated social situation information for organizing and conducting campaign IO activities; to exploit standard or expedient instrument equipment {制式或就便器材 *zhishi huo jiubian qicai*} to assist the other operational strengths in conducting psychological attacks and public opinion propaganda against hostile forces {敌对势力 *didui shili*} and trouble-making groups {*naoshi qunti*}; to adopt effective measures to assist-support the joint campaign large formation's other operational strengths in doing well in IO support work; and to assist in doing well in the security and safeguarding {*anquan baowei*} work for military and civilian information systems.

VII. Missions of the local IO strengths…76

The main missions of the local IO strengths are as follows: to acquire intelligence information, so as to provide intelligence assisting support for joint campaign IO; to exploit means such as radio, TV, newspapers and magazines, and the Internet {*hulianwang*} to assist the joint campaign large formation in executing psychological attacks against the enemy, and in jamming and sabotaging the enemy's political, financial, and public opinion propaganda information systems, to weaken the enemy's war potential {*zhanzheng qianli*}; to adopt measures such as information deception, network protection, and information security [INFOSEC] secrecy {*xinxi anquan baomi*} to protect the security of civilian information systems which assist-support joint

campaign large formation operations; to assist in doing a good job of military information system security; to adopt multiple methods and means to counter the enemy's psychological attacks, and enhance popular sentiment and morale {*guwu minxin shiqi*}; and to assist-support the joint campaign IO logistics {*houqin*} and equipment support work.

Section 4: Organizational Grouping {*bianzu*} of Joint Campaign IO Strengths…76

The organizational grouping of joint campaign IO strengths usually has an organizational grouping form flexibly {*linghuo*} determined in the campaign preparations phase by the IO commander {*xinxi zuozhan zhihuiyuan*}, based on situations such as the general campaign intent {*zongde zhanyi yitu*}, IO intention, battlefield IO posture {*taishi*}, and our military's campaign IO strength composition. **[end of page 76]** It must accomplish mutual adaptation to the campaign scale and campaign pattern, mutual adaptation to the IO missions undertaken by the units, mutual adaptation to the IO capability of the units, mutual adaptation to the campaign organizational grouping requirements, and mutual adaptation to the battlefield environment. From the viewpoint of the needs and requirements of the joint campaign patterns and IO activities which our military can implement in the future, usually there will be two organizational grouping forms. The first is organizational grouping per service and arm {*an junbingzhong bianzu*}, while the second is organizational grouping per operational group {*an zuozhan jituan bianzu*}.

I. Organizational grouping per service and arm…77

IO is an important activity within joint campaigns. Under the usual circumstances, it is composed of a series of interrelated {相互联系 *xianghu lianxi*} ground, air, and sea IO activities. This objective situation requires us from a macroscopic {*hongguan*} standpoint to carry out unified organizational grouping of the IO strengths within joint campaigns, i.e., to perform organization grouping of IO strengths per service and arm.

(1) Organizational grouping of Army campaign large formation IO strengths

The Army campaign large formation IO strengths generally include the IO strengths of units in group armies of the Army {*lujun jituanjun*}, in the Army aviation forces {*lujun hangkongbing*}, and in the related arms {*bingzhong*}. According to the IO means, they can be organized into a certain number of sub-groupings {*fenqun*}, usually including the following: IO reconnaissance sub-groupings, EW sub-groupings {*dianzi duikang fenqun*}, and electronic camouflage and deception sub-groupings. An IO reconnaissance sub-grouping is composed of EW reconnaissance {*dianzi duikang zhencha*} units (elements) and computer network reconnaissance {*jisuanji wangluo zhencha*} units (elements). An EW sub-grouping is composed of electronic jamming units (elements). Based on operational needs and requirements or the equipment's technical characteristics {*xingneng*}, it can be organized into a short-wave communication jamming grouping {*duanbo tongxin ganrao qun*}, air defense EW

grouping {*fangkong dianzi duikang qun*} (ground-to-air radar jamming grouping {*diduikong leida ganrao qun*}), ultrashort-wave communication jamming grouping {*chaoduanbo tongxin ganrao qun*}, ground-to-ground radar jamming grouping {*diduidi leida ganrao qun*}, and EW reserve forces {*dianzi duikang yubeidui*}. An electronic camouflage and deception sub-grouping is composed of electronic camouflage and deception units (elements).

(2) Organizational grouping of naval campaign large formation IO strengths

Naval campaign large formation IO strengths generally include submarines {*qianting*}, surface ships {*shuimian jianting*}, **[end of page 77]** naval aviation forces {*haijun hangkongbing*}, and naval marine forces {*haijun luzhandui*} IO strengths. According to the IO means, they can be organized into a certain number of sub-groupings, usually including the following: IO reconnaissance sub-groupings, EW sub-groupings, electronic camouflage and deception sub-groupings, and entity destruction sub-groupings {*shiti cuihui fenqun*}. An IO reconnaissance sub-grouping is composed of electronic reconnaissance ships {*dianzi zhencha chuan*}, aviation electronic reconnaissance {*hangkong dianzi zhencha*} units (elements), sea early warning patrol {*haishang yujing xunluo*} units (elements), EW reconnaissance units (elements), and computer network reconnaissance units (elements). An EW sub-grouping is composed of ground, air, and sea EW units (elements). Based on operational needs and requirements, it can be organized as follows: a naval operational formation electronic jamming grouping {*haishang zuozhan biandui dianzi ganrao qun*}, seacoast EW grouping {*haian dianzi duikang qun*}, air assisting-support EW grouping {*kongzhong zhiyuan dianzi duikang qun*}, and EW reserve forces. An electronic camouflage and deception sub-grouping is composed of angular-reflector ship {*jiaofanshe ting*} units (elements) and electronic deception and camouflage units (elements). An entity destruction sub-grouping is composed of hard-kill strengths {*ying shashang liliang*} for IO, as well as non-professional IO strengths undertaking hard-destruction operational missions.

(3) Organizational grouping of Air Force campaign large formation IO strengths

Air Force campaign large formation IO strengths generally include the IO strengths of aviation force {*hangkongbing*} and surface-to-air missile [SAM] units {*dikong daodan budui*}, and of antiaircraft artillery [AAA] {*gaoshe paobing*} and early warning and detection {*yujing tance*} units, which according to their IO profession can be organized into a certain number of sub-groupings. These usually include the following: IO reconnaissance sub-groupings, EW sub-groupings, and entity destruction sub-groupings. An IO reconnaissance sub-grouping is composed of aviation force electronic reconnaissance units (elements), early warning and command aircraft {*yujing zhihuiji*} units (elements), EW reconnaissance units (elements), and computer network reconnaissance units (elements). An EW sub-grouping is composed of ground and air EW units (elements). Based on operational needs and requirements, it can be organized as follows: an air assisting-support jamming grouping {*kongzhong zhiyuan ganrao qun*}, an air defense EW grouping {*fangkong dianzi duikang qun*}, and EW reserve forces. An

entity destruction sub-grouping is composed of hard-kill strengths for IO, plus non-professional IO strengths undertaking hard-destruction operational missions.

(4) Organizational grouping of Second Artillery Corps campaign large formation IO strengths

Second Artillery Corps campaign large formation IO strengths, according to their IO professional means, **[end of page 78]** can be organized into a certain number of sub-groupings. These usually include the following: IO reconnaissance sub-groupings, EW sub-groupings, electronic camouflage and deception sub-groupings, and entity destruction sub-groupings. An IO reconnaissance sub-grouping is composed of EW reconnaissance units (elements) and computer network reconnaissance units (elements). An EW sub-grouping is composed of EW units (elements). Based on operational needs and requirements, it can be organized as follows: an air defense EW grouping, an E-O warfare grouping {*guangdian duikang qun*}, a communication warfare grouping {*tongxin duikang qun*}, and EW reserve forces. An electronic camouflage and deception sub-grouping is composed of electronic camouflage and deception units (elements). An entity destruction sub-grouping is composed of hard-kill strengths for IO, plus non-professional IO strengths undertaking hard-destruction operational missions.

The above professional IO groupings of the various services and arms are mainly used for assisting support to the operational activities of the root service and arm.

II. Organizational grouping per operational group…79

In order to even better carry out scientific combination of the joint campaign IO strengths, seeing that all strength essential factors bring into play the optimal superiority {*zuijia youshi*} will boost integrated-whole operational capability {*zhengti zuozhan nengli*}. The joint campaign IO-strength task organization form, often based on the specific campaign's nature and missions, has an organizational grouping of a number of interrelated operational group IO groupings {*zuozhan jituan xinxi zuozhan qun*}. Under the usual circumstances, they can be organizationally grouped into joint campaign directly subordinate IO groups (groupings) {*jituan (qun)*}, Army operational group IO groupings, Air Force operational group IO groupings, naval operational group IO groupings, missile strike group {*daodan tuji jituan*} IO groupings, and special operations group IO groupings. The organizational grouping into the above various group IO groupings is one which sets out from the general situation of the joint campaign IO strengths to carry out a conception [vision] {*shexiang*} and give it consideration. During the actual organizational grouping, it is uncertain {*bu yiding*} that every campaign's IO must organizationally group this many group IO groupings; it could be less than, but also could exceed this scope, and is flexibly determined based on the specific situation of campaign IO.

(1) Joint campaign directly subordinate IO groups (groupings)

The joint campaign directly subordinate IO groups (groupings) usually have a main task organization of General HQ attached and **[end of page 79]** theater directly subordinate IO units, as well as some information offense units of the various services and arms. They mainly include EW units, network warfare units, PSYWAR units, and electronic camouflage units, as well as local IO strengths, and are directly controlled and employed {*zhangwo shiyong*} by the joint operations command {*lianhe zuozhan zhihuibu*}. Usually they are organizationally grouped into an IO reconnaissance grouping, electronic jamming grouping, satellite warfare grouping {*weixing duikang qun*}, early warning aircraft warfare grouping {*yujingji duikang qun*}, anti-radiation attack grouping {*fanfushe gongji qun*}, computer network warfare grouping {*jisuanji wangluozhan qun*}, special attack grouping {*tezhong gongji qun*}, electronic camouflage and deception grouping, and IO reserve forces.

(2) Land operational group {*lushang zuozhan jituan*} IO groupings

These have a task organization of IO units (elements) of the participating group armies of the Army or of its directly commanded related services and arms. They carry out land IO missions, to assist-support land operational activities. Based on needs and requirements, they can be organizationally grouped into a land attack group {*lushang gongji jituan*} IO grouping, land staunch defense group {*lushang jianshou jituan*} IO grouping, land containment group {*lushang qianzhi jituan*} IO grouping, and land maneuver operational group {*lushang jidong zuozhan jituan*} IO grouping. The size of each group's IO strength is determined by watching the missions undertaken.

(3) Naval operational group {*haishang zuozhan jituan*} IO groupings

These have a task organization of the Navy's participating main IO strengths. They mainly undertake [missions to] seize and maintain information dominance, and carry out sea campaign assisting support and screening {*haishang zhanyi zhiyuan yu yanhu*}. Specifically they can, based on the mission, be organizationally grouped into a sea campaign screening (seizing sea dominance {*zhihaiquan*}) group IO grouping, in-advance minesweeping and obstacle elimination (obstacle laying) force-strength group {*yuxian saolei pozhang (bushe zhang'ai) bingli jituan*} IO grouping, and naval fire strike group {*haishang huoli daji jituan*} IO grouping.

(4) Air operational group {*kongzhong zuozhan jituan*} IO groupings

These have a task organization of the participating Air Force and naval aviation forces' {*kong, haijun hangkongbing*} main IO strengths, and their main mission is to assist-support the air operational group in seizing and maintaining air dominance/supremacy {*zhikongquan*}. Specifically they can be organizationally grouped into a strike force-strength group {*tuji bingli jituan*} IO [grouping] and screening force-strength group {*yanhu bingli jituan*} IO grouping.

(5) Missile operational group {*daodan zuozhan jituan*} IO groupings

These have a task organization of the participating operational and tactical missile units' {*zhanyi zhanshu daodan budui*} IO strengths. Their main **[end of page 80]** mission is to screen the security of the missile launch positions {*daodan fashe zhendi*}.

(6) Special operations group {*tezhong zuozhan jituan*} IO groupings

These have a task organization of the special IO units (elements) of all services and arms. Within operations they can be organizationally grouped into a certain number of air, sea, and land special operations groupings {*tezhong zuozhan qun*}, to conduct special IO reconnaissance and special information attacks {*tezhong xinxi gongji*}. **[end of page 81; end of chapter]**

Chapter 5
Targets of Joint Campaign Information Operations…82

Targets of joint campaign information operations are the targets for attack in information operation activities. Determination of the targets of information operations is one of the important substances of information operations decisions made by joint campaign information operation commanders and their command organizations and it is an important basis for the commander's scientific decision and effective plan. Accurate selection and attack of targets in information operations are prerequisite for seizing partial control of information power in a joint campaign.

Section 1: Principle in Selection of the Targets of Joint Campaign Information Operations…82

The selection of the targets of joint campaign information operations should handle the following points in addition to adhering to the general principles in selection of operation targets.

I. Concentrate on the overall situation and hold on to the key point…82

One must unitarily take on the overall situation of the operation and select the key targets that are favorable to achieving operational intent and speeding up the operational process when selecting the targets in information operations. Through the attack of information operations targets, it will create a domino operational effect, break down the enemy's entire structure, and maximally weaken the enemy's overall operational capability. Correct selection of targets can guarantee accuracy in information attack and benefit speedy achievement of the operation goal.

In selection of information operations targets, it must first, obey the requirement of servicing the overall situation of the joint campaign operation. The policy requirement must be closely surrounding the campaign intent, focusing on the overall situation of the campaign, and having a handle of the selection of the targets. It must plan the information operations activities starting from the overall situation and determine information operations attack key point in order to really express the overall power of the joint campaign operation. Second, it must be favorable to speeding up the operation process. It should select and attack the vital point in the enemy's operation information system, use this vital point to defeat and collapse the enemy's overall situation, and achieve the goal of prompt military decision. For example, one can effectively take away the enemy's operation measure, speed up the operation process, shorten campaign continued time, and quickly achieve the goal of the campaign or war by attacking the key parts of the enemy's command and control system and damaging the enemy's perception and judgment capability on the battlefield situation.

II. Stand by one's own capability to precisely select targets…83

When selecting information operations targets, we must base it on the objective reality that our military information operation measure is relatively insufficient and we must depend on our information operations reconnaissance and information attack capability to precisely select the category, quantity, and scale of the information attack target and use the lowest cost, highest efficiency, and maximum limit to damage the enemy's information and information system effectiveness and achieve the operation goal.

In selection of information operations targets, it must first, have a handle on our military information operation capability. Starting from the overall weapon and equipment capability for our military to participate in war, we should comprehensively analyze the sustained time of information attack and operation space and possible result and accurately handle the relationship between necessary and possibility. Second, it should have a handle on the enemy's information operation capability. We should comprehensively understand the category, quantity, function and deployment, military strength, echelon, command system, and operation deployment of the enemy's information operation system and equipment, as well as their operational capability and investable combat forces. Third, it should stand by the idea of defeating the superior with the inferior. Starting out from the actual situation that our military specialized information operation power is relatively weaker, we should stand by our inferior information attack weapons and equipment to strike the enemy's information system; utilize various measures to carry out all-direction, multi-dimension information attack against the enemy; form a comprehensive superiority by cleverly combining soft strike and hard destroy, physical attack and psychological attack; and damage the enemy's information and information system effectiveness with the lowest cost, highest efficiency, and maximum limit to achieve operational goal.

III. Comprehensive analysis and optimum selection of the targets…84

When selecting information operations targets, we should carry out observation and study of multi methods, multi levels, and multi angles; have a handle on the essence in target selection and contradiction in different levels; and optimize the selection of the best attack targets to seek the best effectiveness in target attack.

In selection of information operations targets, it is first, a combination of qualitative analysis and quantitative analysis. Qualitative analysis is to determine the effect caused by carrying out information attack on a target. Quantitative analysis is to provide the basis and material for qualitative analysis. The quantitative analysis result of information operation target selection must still, at the end, be expressed by qualitative analysis. Therefore, it should use qualitative analysis as the main thing to achieve the perfect unification of qualitative analysis and quantitative analysis and raise the scientific nature of information operations target selection. Second, it is the combination of macro-analysis and micro-analysis. Macro-analysis is to fully consider the inner connection and

transformation among all factors that affect the overall situation in the operation and seek the vital target that has decisive effect on the overall situation as the attack object. At the same time, we should also carry out micro-analysis on the target system to find the vital part and attack point and thus, achieve the "domino" effect of "striking one point to break down the entire situation" through information attack of the "vital part." Third, it is a combination of static analysis and dynamic analysis. Static analysis can have a handle of the basic information of a target, understand the general condition of a target to get the general conclusion in peacetime conditions, and provide reference for target selection in wartime. The conclusion of static analysis often cannot keep up with the changes in operation rhythm, so, to a very large degree, it must depend on increasing the dynamic analysis capability to be the answer. Based on the changes of operation task, operation action, operation stage, and operation opportunity, it analyzes the possible development of the relevant factors in information operations target selection, seeks the relatively certain factors under the uncertain environment, and increases the accuracy and timeliness of information operations target selection.

IV. Alteration due to situational changes to flexibly select targets…85

When selecting information operation targets, we should base it on the changes in the objective situation, focus on the nature and operational state of the attack targets, and flexibly select targets based on the different situations and activities that appear during the process of attacking the enemy's targets to timely adjust the attack targets, so the target selection is suitable with the activity characteristic and concrete situation of the targets.

In selection of information operations targets, one should first, closely pay attention to the changes in the enemy's situation. One should timely keep track of the development and change in the enemy situation when selecting targets in information operations, that is to pay attention to changes in operation targets, situational changes of the enemy targets, attack result of the targets, and overall changes of the enemy situation to achieve anticipation of the enemy first and advanced preparation. Second, one should have an overall handle of the changes in our own situation. One should flexibly ascertain the scope of information operations targets and rationally determine the category and quantity of information operations targets according to the changes in operational tasks and operational capability. One should analyze the situation in completion of tasks that are relevant to friendly troops and the existing issues in operation coordination, and also foresee the difficulty that may occur in order to make information operations target selection be coordinated with the relevant friendly situation. Third, one should take the initiative to adapt to the changes in the battlefield environment. One should accurately have a handle on the characteristic and pattern of the battlefield information environment, weigh the advantages and disadvantages, and have a handle of the development trend through investigation and study of the battlefield information environment and then actively adapt to and use the changes in the battlefield environment to increase our military's adaptability to the battlefield environment.

Section 2: The Basis for Joint Campaign Information Operation Target Selection…85

Under the general situation, joint campaign information operations target selection should consider factors such as information operation intent, information operations power, target intelligence, target value, battlefield information environment, and operation timeline.

I. Operation intent…86

Joint campaign information operation intent is the basis for information operations activities that have reflected the most basic intention and concept for the commander to complete the information operations tasks and also is the fundamental basis for information operations target selection.

Operation intent determines the general attack target, not only it relates to the entirety and accuracy in information operations target selection, but also the result of the operation; therefore, selection of information operations targets must be carried out by closely revolving around the operational intention from the higher up. One must clearly be assured of the concrete operational purpose and responsibility in each stage and each time of the campaign and be certain of the information operations targets in each stage and each time of the campaign. During the Gulf War, Kosovo War, and Afghanistan War, in order to reach the goal of paralyzing the enemy's operational system, the US military always made the enemy's command and control center and communication and reconnaissance early warning system the "key points" of its strike when selecting striking targets and making the enemy's operational system to become paralyzed so that it was able to control the battlefield situation, lead the combat development, and lay down a solid foundation for the final victory in war.

II. Operation power…86

Operation power generally indicates the total of factors such as personnel carrying out the operation and weapons and equipment and it is the main body for pursuing operations and material basis for all activities in the battlefield. All expected results of operation target selection in the battlefield must be realized through the implementation of operation power.

Operation power is the material basis in target selection. High-tech weapons and equipment that use information and information technology as the core have become an important symbol to measure the strength or weakness of operation power and have become the objective factor in restricting target selection and also drawing effect on target selection. The strength or weakness of operation power directly relate to the ability to attack a target, attack what target, and achieve what kind of result, and it is an important basis and prerequisite to information operations target selection. For example, if the power is clearly stronger than the enemy military, then one can willfully select

attack targets based on operation intent; on the other hand, if the power is not sufficient, then one can only select some targets that are less difficult and suitable for one's capability. It is only when operation power is transformed into actual operational capability that it can be fully effective in operation and this transformation involves many objective factors. During operations, accurate operation direction combined with favorable battlefield space and time factor could make the party with weaker operation power to gain initiative and finally defeat the strong one and these types of example in the past were many. Therefore, we generally should comprehensively consider these factors when carrying out target selection from the angle of operation power.

III. Target intelligence…87

Accurate selection of information operations targets must rely on first hand target intelligence and then carry out accurate analysis and judgment and have a control of the battlefield situation and the enemy's activity pattern to correctly select operation targets and make correct operation determination.

Target intelligence under informatory conditions has become the prerequisite of information operations target selection. Accurate analysis and utilization of a large amount of target information can provide support to drawing up information operation target decision plan. Six months prior to the Gulf War, with advanced reconnaissance technology and after a long period of thorough and detailed information operations reconnaissance, the multi-nation troops knew the target intelligence such as operational system, frequency, and position of almost all electronic facilities in the radio stations, radar, guided navigational facilities and missile guidance systems of the Iraqi military as the palm of their hands and made good preparation for a scientifically implemented target decisions and the first round precision strike and information attacks after the war started.

Information operations target intelligence must be able to reflect the truth of target and accurate situation and provide accurate data and objective judgment. More accurate target intelligence will make the target selection more precise; while incorrect even wrong intelligence would lead information operations target selection onto a wrong path. The target category that target intelligence is involved in must fulfill the intelligence requirements of target selection and it is without any meaning to provide some target intelligences that are outside the scope of information operations target selection. Under informatory condition, the battlefield situation changes swiftly and operation targets are in fierce dynamic changes, so target intelligence must reflect the target condition in real time in order for target selection to follow the development and change in battlefield rhythm and battlefield situation. The higher the value of target intelligence is, the better the quality of target selection becomes.

IV. Target value…88

Target value indicates the effect and position of a target on a specific battlefield and is a sort of comprehensive index used to describe the necessity to adopt information

operations attack activities against battlefield targets under a specific condition, and it also indicates a certain fulfillment of targets in the requirement of information operations. The source of value comes from targets and targets provide value, and the target value in information operations target selection should be as mutually consistent with actual value as possible.

The fundamental standard of information operations target selection is target value and the core issues to be resolved are mainly two and they are the issues of "do we want to do it {要不要 *yao bu yao*}" and "can we do it {能不能 *neng bun eng*}." The first one is the issue of wanting to resolve the necessity of target attack, while the other one is the issue of resolving the feasibility of target attack.

The magnitude of target value is an important content of target selection and is a certain fulfillment for operation requirements. Information operations target selection is to assess target value and further determine the precedence of attack through establishing a certain standard. Since information operations targets change frequently and are in various forms, furthermore, the factors that affect target value are many; so, how to measure target value with relative scientific and integrated standards has become the key issue urgently waiting to be resolved in information operations target selection. Currently, the indices for measuring target value are mainly: target's importance, which is the position and effectiveness of target in the entire operation system; target's threat, which is the degree of obstruction to our operation activities and level of threat to our security from the target; and target's strike effectiveness, which is the degree in destroyable and recovery of the target. On this basis, it is important to determine index value and index power and finally combine calculate the index value to form a target value rank.

V. Battlefield information environment…89

The battlefield information environment is the general term for various situation and condition in informatory battlefield and its surrounding that affect information operations activities. It is the basis for organizing and carrying out information operations and an important factor for restraining information operations activities. Each category of target in information operations is located in the battlefield information environment and cannot avoid both active and passive influences from the battlefield information environment. Accurate and appropriate amount of information in the battlefield information environment can help the analysis of information operations targets, rational selection and determination of information operations targets, and making close to real-time reaction on the selected targets. Inaccurate and excessive amount of information in the battlefield information environment is not favorable to overall analysis and accurate handling of the situation on the targets and making a scientific decision on the targets.

Under informatized conditions, the operation rhythm quickens; the battlefield situation changes frequently; the undetermined factor increases; the amount of battlefield information increases greatly; the difficulty of handling information increases; all links

such as collection, transmission, handling, and utilization of information will be affected in different degrees; and a tiny error in any one link may lead to serious slip ups. When selecting information operations targets, one should use obtaining a large amount of accurate and timely information as the basis and also speed up the selection rhythm to meet the changes of the battlefield situation, so there is great challenge in the time effectiveness and accuracy of target selection. How to overall understand the battlefield situation and further coordinate information operations target selection with the battlefield reality are the key issues that joint campaign information operations target selection must resolve.

VI. Operation timeline…89

The operation timeline is the reflection of operation activity continuity and also the format of operation activity existence. Any operation activity must proceed in a specific of time and when selecting information operations targets, anyone who wins the time wins the initiative. During information operations target selection, it would have important meaning on increasing the result of target selection and attack if one fully utilized one's own usable time to make a decision and act before the enemy. The US military focused on time effectiveness when carrying out joint target selection and strike by emphasizing "targets that are time sensitive" that is "those targets that cause (or will soon cause) danger to one's own troops and must be taken care of immediately, or those temporary targets that are worthy and will soon disappear," and stipulated in detail the items that should be considered on targets that are time sensitive. On the informatized battlefield, the operation action, force deployment, and operation target of the opposing parties are in dynamic changes, so information operations target selection must keep up with the fast rhythm demand of the war, be good in taking advantage of war opportunity, and distinguish the enemy's movement with sharp observation to discover and catch the smallest unusual phenomenon and sign, predict the situation development and change, timely change the attack targets, and achieve the goal of changing as the enemy, changing prior to the enemy, and controlling changes with fast action. We should quickly identify and attack those technical jamming targets such as maneuvering, camouflage, concealment, and deceiving before the enemy is able to use them, so we can achieve the expected result.

Section 3: Categorization of Information Operations Targets…90

Information operations target category is the partition applied to the types of information operation targets. To scientifically categorize the information operations targets is the prerequisite and foundation for studying information operations target selection in depth and also the objective requirement for closely combining the theory and practice of information operations target selection. Based on different standards, we can categorize information operations targets from different sides.

I. Categorization based on space and location of targets…90

According to the space and location of the targets, we can divide information operations targets into ground targets, water (above and below) targets, and air (space) targets.

Ground targets mainly indicate the targets that use land as the space of their operation activity such as ground radar stations, ground microwave relays communication hubs, ground command information systems as well as other vehicular and stationary information systems and facilities. Land space is the first dimensional space for military activity and it is the starting point and ending point of the other spaces activities; therefore, land targets constitute the main entity of operation targets. Following the fast development in science and technology, the operation space is constantly expanding and the position of water targets and air targets are also becoming more profound in modern war. Water targets and air (space) targets are the second dimension and third dimension respectively and space targets have been gradually developing after new operation measures such as naval vessels and airplanes (satellites) appeared and are used in large quantity in wars. Water (above and below) targets include mainly all types of vessel carrier information systems and facilities and air (space) target includes mainly all types of airplane carrier (satellite carrier) information systems and facilities.

II. Categorization based on attack measure…91

The attack measures of information operations mainly include electronic attack, network attack, and psychological attack. Starting from this angle, one can divide the information operations targets into electronic attack targets, network attack targets, and psychological attack targets.

Electronic attack mainly includes electronic jamming, counter-radiation weapon attack, and special information warfare weapon attack and it emphasizes more on the weakening and damaging of information collection and transmission links and the targets are mainly all types of electronic information systems such as early warning detection systems, command and control systems, and communications systems. Network attack mainly includes information stoppage, network infiltration, and virus attack and they mainly damage the enemy's information management through searching of network's "loophole" and "backdoor" and the target is mainly network type information systems. Psychological attack mainly includes psychological propaganda, psychological deception, and psychological threat.

III. Categorization based on the importance of target…92

In this categorization, information operations targets can be divided into core targets, key targets, and general targets. A core target is the enemy's target that has important meaning and with major supporting effectiveness such as the enemy's command and control system. The number of core targets is limited but with great value

and once attacked, they may cause the enemy's information to be paralyzed and the operation system to collapse. A key target is an enemy's target with important effect and rather great influence. A general target is a target with general effect and least influence. It is necessary to point out that core targets, key targets, and general targets are often relative and conditional and under a specific situation, they can mutually transform.

IV. Categorization based on targets attack sequence…92

Based on targets attack sequence, it can be divided into primary attack target, follow-up attack target, and sustained attack target. A primary attack target is a target that should be attacked first based on operation requirement and generally is a target with strong time effectiveness or great effect and the highest importance in follow-up operation activities. A follow-up attack target is an attack target that is relatively behind in time sequence, relatively speaking, comparing with a primary attack target and generally is the second and third batch target. A sustained attack target is a target that requires close attention and is always maintained in attack condition during all process or most of the time in information operations such as the enemy's command information system.

V. Categorization based on the composition of target…92

Information operations is an action adopted to weaken and damage the enemy's information and information system, and at the same time, protect one's own information and information system, so an information operation target mainly is composed of information and an information system; therefore, we can divide the targets into information and information system based on composition of the target.

An information system is the general term for a system especially used to collect, store, handle, transmit, manage, and utilize information. An information system has many categories and they are the strategic information system, campaign information system, and tactical information system if divided based on their level and scope of utilization, and intelligence reconnaissance system, early warning detection system, command and control system, communications system, and information operation system if based on their function and usage.

Section 4: Joint Campaign Information Operation Target Selection Procedure…93

The general procedure of joint campaign information operations target selection: accumulation of target information, analysis and edition of intelligence; learn the operation intention, understand the information operations task; collect battlefield intelligence, identify target information; analyze target characteristics, predict target inventory; determine target inventory, propose decision-making suggestion.

I. Accumulate target information, analyze and edit intelligence…93

As the first step of information operations target selection, accumulate target information and analysis and edition of intelligence must be developed around satisfying the requirements for information operations target selection.

First is to collect wide a variety of target information. The wide collection and accumulation of target information are to collect and be in control of the information operations intelligence information of the advanced nations and neighboring nations and regions and be in control of their radar, communications, electronic warfare, and network warfare units, as well as their relevant deployment, authorized strength sequence, tactical technical function, working patterns and development actions, and operation ideological principles. Second is to collect the focal point of target information. That is one should analyze the make-up and tactical technical parameters of the major opponent's information system in information operations and one must especially focus on checking the enemy's operation structure, troop deployment, and major operation method to provide strategic intelligence to one's own information operations and comparatively macro intelligence information support to information operations target selection. Third is to analyze and reorganize target intelligence. That is one should put together the goal of information operations activities with all the collected target intelligence information and material and carry out synthesis, analysis, assessment, and approval. One should pay attention to analyze overall and in detail the intelligence information that are collected through all channels and truthfully come out with the correct analytical conclusion to avoid prejudice and wishful thinking and result in incorrect judgment.

II. Learn the operation intention, understand the information operation task…94

Learning the operation intention and understanding the information operations task are to carry out information operations target selection under the direction and restriction of operation intention and operation requirement.

(1) Learning the intention of the higher up

When selecting joint campaign information operations targets, learning the intention of the higher up must focus clearly and accurately on operation goal, operation direction, operation strength, and operation stage. The first one is to clarify the operation goal. Different operation goals lead to different target selection, for example, if our operation goal is to conceal surprise defense, then the selected attack targets are definitely the intelligence reconnaissance system, early warning detection system, and air defense anti-missile system. If our operation goal is strategic threat, then the attack targets are generally the targets that can create major political influence such as the government network and the electric power system. The second one is to clarify the operation direction. During operation, the major operation direction should be favorable to achieving the intention of the higher up, reaching the operation goal, winning the primary war, and development afterward. The third one is to clarify the operation strength that is

how much operation power to put in and what military forces are deployed in operation to fully display the effectiveness of different military forces and weaponry in order to show the greatest overall strength of the operation system. The fourth one is to clarify the operation stage. One can divide the entire operation into several closely connected stages according to implementation sequences and based on task, striking target, or main operation activities of each military service. The task, target, and operation activity on each stage are often different.

(2) Understanding the information operations task

One should first be clear of the time, location, deployed unit, adopted method, organized action, action's target, the number of the unit's military force in this action, the weapons and equipment used, the units to be coordinated with, the task to be completed, and the requirement after the task is completed that the higher up has in mind. One should focus on the information operations task, connect the order and direction of the higher up to proceed with thinking and consideration, and accurately hold on to the intention of the higher up and the task of one's own unit.

III. Collect battlefield intelligence, identify target information…95

Collecting battlefield intelligence and indentifying target information are to try its best to timely understand and be in control of the situational changes on the battlefield and identify the target information based on intelligence accumulation in peacetime, making the information operations target selection to be built on the foundation of true and objective target information.

(1) Clarifying the necessity for battlefield target intelligence

It is mainly to understand: the technological level; operational structure; special parameter; and tactical function, deployment, style number, quantity, and working method of current enemy; the organization mechanism of current enemy's electronic warfare, network warfare, and psychological warfare as well as the authorized strength sequence, personnel, and equipment strength of the corresponding units and the quality in training of the units; and the tactical operation principles, relevant regulations, and the troop utilization situation during operation of the electronic warfare, network warfare, and psychological warfare units.

(2) Clearing the channels for collecting intelligence information

Clearing the channels for collecting intelligence information should start mainly from the following aspects: first is to strengthen intelligence information communication with the higher up and that is to accept the higher up's report on enemy's situation and request the higher up for clarifying the relevant situation. Second is to strengthen intelligence information communication with the intelligence departments. The information operation intelligence departments should provide a comprehensive enemy's

situation report that includes mainly the enemy's situation, final conclusion on the enemy's situation, and suggestions on events to be checked and the organization of intelligence reconnaissance. Third is to strengthen intelligence information communication with the subordinates and friendly neighboring nations, that is to put together the scattered intelligence collected by the subordinates and turn them into intelligence required for target selection through comprehensive analysis and handling. Fourth is to utilize the relevant intelligence collected from other channels that is the intelligence through questioning local units, local relevant departments, as well as reservist, militant, and the public.

(3) Identifying intelligence information of targets

All-position study of targets' intelligence, generally, should start from the following aspects: first is to identify the function of targets, that is, can the attack of this target break down the enemy's operation system, affect the campaign overall situation, and directly achieve one's own operation goal. Second is to identify the target's structure, that is, to ascertain the target's fatal part through studying the hierarchical structure and relevant structure. Third is to identify the composite distribution of the target that is to mainly clarify the category of the target and its concrete composition. Fourth is to identify the quantity, degree of threat, and degree of destructibility of the target.

IV. Analysis of target's characteristic, preliminary drafting of the target's detailed list…96

It is mainly to carry out comprehensive analysis from the importance of all targets in the enemy's operation system, threat to our operation action, and feasibility for implementing target attack; analysis of sequence on targets; and preliminary planning of the information operations target list.

(1) Analysis of the importance of the targets

The importance of the targets is reflected through the target's structure, function, frequency spectrum, make-up, and capability.

1. Analysis of target's structure

Target's structure is an organic body composed of many mutually connected target systems and with many existing starting, connecting, and supporting points. If one can find the structural connecting point of the enemy's target system and carry out effective attack, then one can achieve the effect of "hitting the point to break the whole" and "pulling a hair to activate the whole body." The enemy's command and control system, intelligence warning system, and communications system are the connecting points in attack target's system structure. During the Bekaa Valley war in 1982, from analysis, Israel discovered that the control center and radar system were the connecting points in target structure of the Syrian air defense operation system and thus drew up an

operation plan of attacking Syrian air defense radar first. In a short six minutes, the 19 "SAM-6" missile base that Syria had worked very hard to build up for 10 years, and spent US$200 million on, had been blown to dust.

2. Analysis of the target's function

Analysis of the target's function is analysis of the relationship between the tasks of all substances in the information system. From the angle of operation utilization, one should mainly analyze the following functions: first is the information collection function that mainly has a warning detection system, intelligence reconnaissance system, and some reconnaissance and warning facilities. Second is the information transmission function that has mainly communications systems. Third is the information handling function that has mainly command and control systems. Through analysis of the functions of targets, one can make target selection the "appropriate medicine for the symptom" that is favorable to further analyze the target, thus making target selection much more accurate.

3. Analysis of target frequency spectrum

Through the analysis of the frequency spectrum of targets, one can ascertain the relationship between the working frequencies of all substances in the target system and study the reflective form of the frequency spectrum that is used by the target's electromagnetic radiation. First is the analysis of the scope of frequency used and the scope of frequency used is the area border of frequency that the target signal uses. Second is analysis of the frequency distribution, and the frequency distribution is the distribution situation of target information in the entire frequency area. The major operational frequency scope of an information facility (system) including radar, communications, guidance, friend or foe recognition, wireless detonator, and guidance is between 1MHz to 300GHz. The frequency scope of the optical electronic information facility (system) generally is above 300GHz. The frequency scope of an acoustics information facility (system) is in the scopes of mid-wave, long wave, and super long wave including secondary acoustic wave, acoustic wave, and super acoustic wave sections and it is the major wave section of sonar and underwater navigation and positioning facility operations. Third is analysis of the target's frequency used form. In terms of a modulator type carrier, the frequency used form is the modulating method. The quantity of target's modulating style is specific, such as in communications area, regularly used simulating signals are amplitude modulator and frequency modulator; digital signals are differential phase-shift keying, time differential phase-shift keying, frequency differential phase-shift keying, time frequency differential phase-shift keying, encoding modulator, two-phase phase-shift keying, and four-phase phase-shift keying.

4. Analysis of the target's appropriation

The analysis of the target's appropriation is mainly accomplished through analysis of point position, route, hub, and region. First is the analysis of point position. Point

position is the position in space occupied by various substances of a target system. The information link point has basic space special characteristics and nature such as position, distribution, distance, and neighbor. In operation under informatized conditions, point position is the information that should be first ascertained in command, control, and strike. Second is analysis of the information route. Route can be used to describe the distance relationship, connection relationship, and flowing relationship among the target's information link points. One can further have a handle of the information communications between the important information link points within the scope of a specific area through information route analysis in order to provide an entrance point for information operations attack and the relevant target selection. Third is analysis of hub. A hub is a crossing point with comparatively great value and a prominent position for a large number of routes. The hub for information operation target system should mainly be the location of the information facility (system) that has a comparatively large influence on the military struggle; therefore, the location of a hub generally is also the location of the target selection's key point. Fourth is region analysis. A region is an abstract combination composed of space structures such as point position, route, and hub, and it has specific form, area, and body. Generally, one can divide the category in the target system into core region, important region, general region, bordering region, and unrelated region based on the degree and amount of importance of the hub in the space.

5. Analysis of target's capability

A target's capability is mainly an expressive form of target information strength and generally, it can be carried out through analysis of information transmission capacity, power density, and radiation source data. Information transmission capacity is the largest information quantity that is transmitted within a unit time. Transmission of information cannot leave out the support of the information system. The tasks of an information system are the collection, transmission, storage, and management of information. Power density indicates the capability in a unit area within a unit time: the larger the power density, the stronger the electromagnetic signal. In terms of electronic jamming, insufficient jamming power and power density are very difficult to carry out jamming against a target. Radiation source data is the number of radiation signal sources on the battlefield. Radiation source data within a unit area can reflect the appropriation density of the information facility and the operational condition of the information facility, combine the changing situation of target radiation source data in certain operation region or operation time, and discover the in-depth level dynamic cause of its changes to provide decision-making basis for information operation target selection.

(2) Analysis of the threat from targets

The threat from targets is a prediction on a certain degree of threat from targets and is one of the major bases in selection of information operations targets. It generally includes analysis of the threat effective factor of target, analysis of the threat effective degree of a target, analysis of the threat index of a target, and analysis of the threat level of a target.

1. Analysis of the threat effective factor of a target

The threat effective factor of a target indicates the substance or condition that creates influences on target's threat and is the major data that affects the sequence of an information operations target threat. When analyzing the threat effective factor of a target, one must look into the effective factor in as much detail as possible. Information operations targets can be divided into electronic attack target and network attack targets and electronic attack target can be divided into four categories - radar targets, communications targets, optical electronic targets, and other targets. Based on these, one can list the concrete threat effective factors; for example, the threat effective factors of a target for radar generally are distance, repetitial frequency, carrier frequency, pulse width, antenna bearing change, and radiation capacity.

2. Analysis of the threat effective degree of target

The threat effective factor of a target is the major data that affect the sequence of an information operations target's threat. Every threat effective factor has a corresponding threat effective degree or threat effective degree function and the threat effective degree generally is a whole number between 0 – 100 and the bigger the number indicates the bigger threat effective degree.

3. Analysis of the threat index of a target

The threat index of a target in information operations is a quantitative description of the threat degree of a target in information operations. It is jointly determined by the attributive data (threat effective factor of the target), battlefield environment, and concrete operation goal of the information operations target. The threat index of a target in information operations combines situations such as the target's battlefield environment and concrete operation goal, and based on the combination of each threat effective degree data to obtain the threat index of the target in information operations.

4. Analysis of the threat level of a target

The threat level of a target in information operations is a qualitative description of the threat degree of a target in information operations. The value of the threat level is English capital letters A – E with A being the highest threat level and E being the lowest threat level. The corresponding relationship of the threat level of a target in information operations is as follows:

Threat Index of Target	0 – 19	20 – 49	50 – 69	0 – 84	85 – 100

Threat Degree of Target	E	D	C	B	A
Meaning in Threat Levels	Smallest	Rather Small	General	Rather Big	Biggest

(3) Analysis of the feasibility of target attack

Feasibility analysis in information operations target selection mainly includes analysis of the information operations attack capability, analysis of the target's destructibility, and analysis of the target's recoverability.

1. Analysis of information operations attack capability

Information operations attack capability is the collective expression of the information operation capability and technical expression of the weapons and equipment attack standard, and it requires combined effects and cooperative support from multi aspects. The analysis of the information operations attack capability is connected to multi factors, and the information supporting capability, command and control capability, information operations weapons and equipment system attacking capability, and comprehensive safeguarding capability jointly constitute the information operations attack capability. Each type of capability can be made in detail to a series of concrete indications, for example indications such as battlefield information collection capability can be made in detail to information collection probability, information collection timeline, information collection precision rate, information collection accuracy rate, and information collection area scope. One can obtain the conclusion of each type of capability by carrying out a comprehensive evaluation of the indication of that type of capability.

2. Analysis of target's destructibility

A target's destructibility is the possibility of the target's function being weakened or damaged after the target is attacked. A target's destructibility includes the target's protect capability and the target's defense capability. A target's protect capability is the ability of the target to adopt its protection measure when the target of the attacked party is attacked and it is the protect capability given to the target by outer power. A target's defense capability is the ability that the target has to defend against attack by the opposition. It can be further made in detail to counter precision guidance weapon jamming capability, counter GPS jamming capability, counter friend or foe recognition jamming capability, counter radar jamming capability, counter communications jamming capability, and counter optical electronic jamming capability. With different targets, the attack action, defensive measure, and self defensive nature and measure against the

targets are also different; therefore, in analysis, one must carry out specific analysis on a specific target.

3. Analysis of target's recoverability

A target's recoverability is the target's ability to recover its basic function after being attacked. Starting from the basic component angle of the target, this type of capability can be made in detail to software recoverability and hardware recoverability and through the analysis of these two capabilities, the evaluation can have the recoverability conclusion of the target.

V. Determine target detailed list, propose decision-making suggestion…102

Determining target detailed list and proposing decision-making suggestion are to carry out renewed determination and inspection of the target based on the preliminary drafting target detailed list in order to ensure the accuracy and scientific nature of the target detailed list and on this basis, also propose the relevant decision-making suggestion of the target attack focusing on the target detailed list.

(1) Inspection of the target's information

A target's information is one of the important bases for information operations target selection. Accuracy, timeliness, and completeness are general standards for quality evaluation of a target's information. Therefore, one must start from the accuracy, timeliness and completeness of a target's information when making inspection of target's information.

1. Inspection on the accuracy of the target's information

When making inspection on the accuracy of a target's information, there should be first, a multi-channel testimony. Through tightly combining information obtained by various methods such as satellite reconnaissance, air reconnaissance, sea reconnaissance, land reconnaissance, as well as specialized reconnaissance, and man-made reconnaissance, the true target's information is captured to a maximum degree by mutually testifying and replenishing the collected information. Second, there should be dependable levels that rationally classify the target's information. The target's information should be classified according to its reliability during inspection and they are generally classified into three levels – reliable, quite reliable, and unreliable.

2. Inspection of the timeliness of a target's information

When carrying out target selection, one should always maintain communications with intelligence reconnaissance departments and utilize various advanced intelligence collection, transmission, and handling measures to control the first hand target's

information at the fastest speed within the possible shortest time. One should analyze and be in control of its time effective scope in order for target selection to be coordinated with information time effectiveness.

3. Inspection on the completeness of a target's information

When assuring target's information, one must pay attention to the inspection of information completeness. One should inspect and make clear its basic parameter on a single target and on the target system, one should make sure that there are no missing targets, especially whether or not the information of a core target can satisfy the requirement in information operations attack. At the same time, one should also recognize the scope of strike on target, so target selection is within the specified scope and one must avoid selecting a target that is prohibited for strike.

(2) Evaluation on the effect of a target attack

Evaluation on the effect of target attack, in reality, is the analysis of whether or not the predicted result can be created after an information operation attack is carried out based on the preliminary drafting target detailed list.

1. Evaluation of the political effect

Evaluation of the political effect is an analysis of whether or not it could achieve the result that is favorable in realizing one's own political goal after the target is attacked and of trying its best to lower and weaken the realization of the enemy's political goal. When selecting the information operations targets, one must focus on the analysis of the political effect created by the evaluation of target attack, insist on the uniformity of military goal and political goal, and pursue the maximum military and political effectiveness. The purpose of regional war under informatized conditions is relatively limited; the connection among military, politic, economy, and diplomatic is much closer; the result achieved by military action often is only one step toward the end in political resolution; and at the end, military confrontation will have to return to the method of political resolution. Therefore, evaluation of the political effect, in fact, is analysis and decision of whether or not a "reasonable, favorable, and moral" political result will be created after selecting target and implementing attack.

2. Evaluation of military effect

The evaluation of military effect is an evaluation of whether or not effective system breakdown is created after the attack action was adopted on the selected target. Information operations is a struggle carried out to weaken and damage the enemy's information and information system and at the same time, protect one's own information and information system from being damaged. There is a linking point in the information system that once it is damaged, it would cause a chain reaction and lead to partial and even the entire system to break down, creating a domino effect. It would achieve the

effect of "hitting a point to damage the surface" and "pulling a hair to affect the entire body" when these linking points targets are attacked. For example when the linking point and hub of a battlefield communication system and a battlefield network system are effectively attacked, they could lead to the command and control system, early warning detection system, and weapon and equipment system to be paralyzed and weaken and lower their operation capability.

3. Evaluation of psychological effect

Evaluation of psychological effect mainly is the effect created on the enemy's recognition system after the target is attacked. First of all, one should analyze the effect on the understanding and confidence of the enemy's command personnel; especially carry out evaluation of their understanding, judgment of the situation, decision on action, and determination and willingness to counter attack on battlefield information. Just as the so-called "shoot the horse first and then the rider, catch the head of the gangsters first and then the rest of the gangsters," one should only be in control of the psychological effect of the enemy's command personnel to be in control of the major aspects of the issue. Second, one should analyze the effect caused by the understanding and confidence of the general operation personnel by analyzing, in focus, their operational attitude, operational emotion, operational spirit, and operational will. Third, one should analyze the effect caused by the understanding and confidence of the enemy's public by focusing on the analysis of their attitude and feeling about war. Finally, one should evaluate the psychological effect caused by one's own allies, the enemy's allies, and those who are neutral.

(3) Report the detailed list to the higher up and propose a suggestion for target strike

Under the informatized conditions and with the quickening of operational rhythm, the time for target selection is lessening, the tendency for uniformity of target selection and strike is getting much clearer, and the traditional method of following prescribed order of selection first and then strike can hardly meet the demand for information operations. Therefore, for the convenience of inspection from the higher up and promoting uniformity of target selection and strike, one should not just merely have a simple list of the targets when reporting the target detailed list to the higher up, but should, at the same time, report the relevant suggestions on the basic situation and target strike when reporting the target selection to the higher up.

1. Basic situation of target selection

The basic situation of target selection is a clear and concise conclusive report on the thinking and behavior process of information operations target selection and the purpose is to provide assistance for the higher up inspection department to quickly have an overall control of the target detailed list. Its content mainly includes the major bases, guiding idea and basic principle, major method, key point and difficult issues that are

already resolved, issues waiting to be resolved, and other situation on information operation target selection.

2. Relevant suggestion on the target strike

When reporting information operations target detailed list to the higher up, the purpose for providing a relevant suggestion on the target strike is to make the target detailed list inspection departments understand the thinking of their target selection; at the same time, it also provides a specific reference for adopting strike action against the target. These suggestions mainly include: target attack time – combining operation stage division and proposing the suggestion for the best timing to adopt strike action against the target; target strike force – based on the analysis and understanding of one's own operation force and operation capability, proposing suggestions on the distribution of information operations strike force against the target; and target strike method – focusing on the operation method, characteristic, and special parameters of the specific targets, proposing suggestion on the focal information operations strike method.

Chapter 6
Basic Fighting Methods of Joint Campaign Information Operations…106

Information operations serves as a type of brand new combat form, its content is extremely abundant, and due to the changes in combat principles and combat environments, the fighting methods for the combat process of the information operations are also multivariant, and so they should be based on the tasks and requirements of the information operations. When the time, locations, and enemy situations are suitable, they should flexibly use the corresponding fighting methods and strive for success in the information operations.

Section 1: Establishing the Basic Requirements for the Fighting Methods of the Joint Campaign Information Operations…106

The fighting methods, which are the methods of combat, are an important component of combat theory. Within joint campaign operations in the future, the information technology trends become clearer with each passing day and striving for information dominance becomes more important with each passing day. Based on the tasks and requirements of the Chinese military joint campaign, it involves the research of the basic fighting methods of joint campaign information operations. It has an important significance, with regard to the guidance of the construction of the Chinese military information operations forces, the enhancement of joint campaign information combat training, the increase in joint campaign information operations combat capabilities, and finally, the commanding points and the grasp of the combat initiative that they have in future information technology wars.

Joint campaign information operations are a new style of **[end of page 106]** joint combat operations of the local wars, under information technology conditions, and it includes all of the basic characteristics that protect against the possible operations that could be implemented by the enemy information systems and their facility attacks, and against the possible operations against our information and information systems, as well as the basic characteristics of the integrated duality and methods, the basic characteristics of the developmental trends, etc. When researching the fighting methods of the joint campaign information operations, they must grasp the following points well:

I. The integration of the objective physical foundations and the subjective dynamics…107

The establishment of the fighting methods must be based on a specific physical foundation and at the same time, it also cannot neglect the subjective dynamic of the people. It should also accomplish the integration of the objective physical foundation and the subjective dynamic. With regard to the Chinese military, establishing the fighting methods should be based in the subjective realities of the Chinese military information

operations weaponry, and the basic principles of the fighting methods should be placed on the foundation of the existing information operations weaponry combat skills and functions. It should focus on the possible developments that could occur in the near future, and it should fully bring out the function of the dynamic use of the subjective guidance and the information operations potential of the people's wars and form an entire military force.

II. The integration of the focus on skills and the focus on theory…107

Combat has always been the measure of intelligence and strategy, but in modern advanced technology wars, it has fully realized the determining function of the technology on the fighting methods. On one hand, they must focus on striving to gain the fighting methods for information dominance, starting with technology and research. For example, "node destruction" is an important fighting method for attacking enemy information systems, so what is the structure of the enemy combat systems? Where are the key links for their command information systems? And how do we differentiate them, interfere with them, and destroy them? What are the most effective methods to use to interfere with and destroy them? How do we confirm the attacks were effective? With regard to the substantive nature of these issues, if they are not deeply and technically analyzed, then we are stuck at summarizing the general characteristics and outwardly describing them in a general fashion, which is not effective in solving the issues. On another hand, they must focus on using strategic control and using methods for distributing technology, they must use the "asymmetric combat" that the Chinese military established on the foundation of strategic superiority and the "killer" of the local advanced technology, in order to cope with a strong enemy that is constructing an advanced technology superiority that regards information superiority as the core, and against enemies that implement skillful and flexible asymmetric combat **[end of page 107]**.

III. The integration of the scientific quality and the artistic quality…108

The fighting methods are scientific and they are also artistic. Following the broad use of new and advanced technology that has been given precedence, the extent of the scientific nature has continuously increased. However, after all is said and done, combat is a type of complex, societal phenomenon of intense fighting, and thereby it provides a broad scope of operations for the art of combat. Within the joint campaign information operations of the future, using the unique function of "soft kill" as the preference for striving for information dominance determines that the most appropriate integration is on the emphasis of the scientific nature and artistic quality. There is a complementary relationship between the scientific nature and the artistic quality. The fighting methods of joint campaign information operations include a large amount of standardized, procedural, and logical stable content, and therefore, they must abide by certain scientific principles; furthermore, they also include many non-standardized, non-procedural, and non-logical unstable content, and therefore they must also be adept at being flexible and defeating their opponent by using surprise moves. For example, in the words of our

forefathers: “Carrying out operations is methodical but it does not make laws. War does not make laws and it is methodical.”

IV. The integration of carrying on and development…108

Joint campaign information operations are a combat realm that is in the middle of rapid developmental change and furthermore, the focus of the offensive and defensive technology measures and methods of the information realms is strong, the benefits of the repeated use are low, and these characteristics determine that they must focus on the continuous innovation of the fighting methods. This type of attempt to use the glories of the past wars to re-cast the glories of future ones only results in the regulations of “no longer being victorious,” being defeated. Moreover, during the past exercises of the Chinese military in the past revolutionary wars, a complete set of fighting methods that have been superior, successful, and excellent has been created, its essence has an important guiding significance on fighting in the information realm, and it should combine the new situations in order to creatively carry forward and develop the traditional fighting methods. The information era allows the life cycle of the military theory, which includes the fighting methods within it, to be continuously reduced, it allows for the farsightedness of the urgent requirements for the research of the fighting methods to be moderate, and this puts forth a strong response for a requirement to challenge future combat, and it is also the draw for the requirements of the previous joint campaign information operations weaponry of the Chinese military to develop and to develop the construction of the troops **[end of page 108]**.

Section 2: Joint Campaign Information Attack Fighting Methods…109

Information attack focuses on striving for and protecting information dominance, under the unified command of the joint campaign commanders and their commanding organizations, using specialized information attack forces and non-traditional forces, adopting electronic interference, electronic spoofing, computer virus attacks, and network infiltration, military sabotage and firepower destruction, psychological attacks, and other integrated measures, as well as destroying and weakening the enemy’s information systems, to the maximum extent possible, in order to use effective, active, offensive combat operations. Its basic fighting methods are:

I. Information deterrence methods…109

Information deterrence methods refer to the collective use of a relatively large amount of information attack troops and military equipment in one or several directions, the adoption of electronic feigning, electronic jamming, network attacks, psychological spoofing, anti-chemical destruction and precision attacks, and other measures, as well as other corresponding campaign deterrence operations that create a formidable information attack momentum and form a psychological perspective. It is a type of information attack fighting method that shocks the enemy military, causing the enemy to not dare to hastily conduct operations or it causes the enemy to submit because of their fear. Moreover, with

regard to the military forces and firepower deterrence, information deterrence can achieve the deterrence objectives and it can also reduce the political and foreign affairs combat restrictions. The actual forces that implement formidable information deterrence methods are even more effective, so much so that they can even achieve the objective of "not fighting but being the victims of war." However, when strong forces are faced with the weak they also do not really accomplish anything; they only are adept at transforming from the bad to the good. They transform their inferior position, in general, to a superior position, specifically, and they implement vigorous information deterrence against the enemy. They mitigate or restrict the information superiority of the enemy, which means they do not allow the enemy to achieve the results of "not fighting but being the victims of war," and it also can cause the enemy personnel to generate feelings of fear and panic, which cripples their combat willpower and then they will not hastily conduct operations. During the "Desert Shield" operations in the 1991 Persian Gulf War, the United States military urgently mobilized all types of forces to adjust their troops and send their generals and high officers to the Persian Gulf regions **[end of page 109]**, while they implemented psychological warfare deterrence through all types of news media, where they greatly exaggerated their electronic warfare results and declared that "they were intently focused on the mobilization situation of Saddam's troops." This caused the spirits of the Iraqi military to be at a high point and they were not willing to conduct hasty operations, thereby effectively concealing the dispatch and deployment of the United States armed forces. In the 1960s, when the Taiwanese military was vigorously making preparations to counter large attacks, the Chinese military had defeated the enemy, and through the organization of a large array of electronic feigning activities, they created errors in the assessment of the Taiwanese military situation and they concealed the mobilization of the Chinese military. They could then leisurely complete their countermeasure preparations, which allowed their countermeasure plans to be aborted.

The use of information deterrence methods, one, is the full use of broadcasts, television programs, publications, Internet, and other news media to propagate the outstanding functions of the Chinese weaponry and the mixture of truth and lies about the military strength when assigning the operations, etc., as well as significantly publicizing the preparations of the Chinese information attacks. This causes the enemy officers to have feelings of panic, even to the point of leading to the enemy organizations and agencies being frightened and it shakes their belief in their fighting capabilities. Two, they should flexibly organize the electronic feigning activities, the electronic disguises, and their electronic jamming on the enemy information systems, their network spoofing, and their virus attacks. Three, they should use virtual reality technology to create a formidable Chinese information offensive, supplementing the essential military feigning activities, warning and frightening the other side, and forcing the enemy to give in. Four, they should use anti-radiation guided missiles, anti-radiation unmanned aircraft, etc. They should implement the "eye-gouging military tactics" against the enemy which serve as the early warning survey radar for the "eyes" of the command information systems, and they should use precision guided weaponry to implement their "pinpoint tactics" on the enemy command and control centers, communications centers, computer network nodes, and other strategic point objectives, which increases their deterrence results.

II. Information blocking methods…110

Information blocking methods refers to the collective use of the superior information attack troops, within a specific time, on the enemy electronic information systems in a certain area, to implement a large scale suppression of electronic jamming, which combines the use of radio communication disguise, network spoofing, and other measures. They sever the communications and networks of the enemy with the outside world and they confuse their radar and photoelectricity reconnaissance, and they block the enemy information attack fighting methods of the enemy, within the electronic information realm. The objective of this fighting method lies in severing the full electronic information connection with the portion of the upper level authorities and friendly neighbors **[end of page 110]**, creating a partially closed off status on the battlefield, in order to create beneficial conditions for the Chinese campaign combat groups on the isolated and scattered enemies, to break them up and surround them, and use all types of attacks on them. During the Battle of Stalingrad, the Soviet military, during the implementation of the preparation phase of their countermeasures against the German military and during the execution process, used radio telephones to specially create interference and destroy the information connections between the six groups of German military units that had been surrounded, and the "Don" military groups, so they could obtain the successful experience of using information blocking methods. The Chinese military, during the self-defense war against Vietnam, also successfully used "information blocking" methods and stopped the radio communications between the Vietnamese military artillerymen at the observation posts and the artillerymen in the battlefield, which obstructed their information transmissions.

In order to use information blocking methods, first, they must reasonably determine the blocking objectives. Due to the increase in the degree of transparency of the information technology battlefields, it has caused the information blocking, in its normal significance, to become more and more difficult. Implementing information blocking against the enemy does not mean they seek to obtain full information blocking and restrictions against the enemy, but they should determine the specially designated enemy military targets to block, within the scope of a certain time and space. The second is that they must integrate the use of different types of methods to implement the strict blockages. At the same time as severing the communications with the outside world, they should implement a strong and stifled interference of the enemy electronic information systems, especially the radio communications with the outside world, and they should, based on the fear of the enemy, isolation and aide, contact, and other situations, flexibly adopt radio communications disguises, transmit false intelligence, and other spoofing measures, and then they can draw the enemy into an ambush so they can dupe and mislead them. The third is that they must promptly evaluate and fully use the blocking results. Regardless of what types of information blocking methods they use, they must promptly evaluate the blocking plans and the implementation of results, and based on the requirements, they must promptly adjust their blocking plans and guarantee the continuous blockade of the enemy within that certain time. Furthermore, they must closely coordinate with each of the campaign groups (combat groups) and troops, fully

use the information blocking results, and implement intense surrounding and annihilation of the enemy **[end of page 111]**.

III. Information campaign methods…112

Information campaign methods refers to the information attack fighting methods that use electronic disguises, electronic feigning activities, network spoofing, and other information spoofing methods, to conceal the Chinese campaign attempts, as well as their deployments and operations, to confuse, dupe and move the enemy personnel, to cause the intelligence of the enemy to be inaccurate, and to create mistakes in the assessments and judgments of the enemy, in an attempt to form a favorable condition for the Chinese military or for them to achieve suddenness in their campaign attacks. The information campaign methods are the embodiment and use of campaign stratagems in the information warfare realm. On future information technology battlefields, through each of the types of information campaigns, with regard to the command of the Chinese military strategic superiority, winning the battlefield initiative has an extremely important significance.

With regard to using the information campaign methods, first of all, it is based on the overall campaign situation. The information campaign methods are an organic component of the campaign rally, and they must obey the campaign objectives, in order to coordinate hiding the truth with the combat operations, and to coordinate exposing the falsities with the combat situations. When it is used in each operation of the information campaign, it must comply with the fundamental principles of the campaign operations, it must accomplish being lifelike in shape and form, and it cannot show its weak points. The second is that it must focus on integrating the campaigns. The information campaigns must acquire the predetermined results, and looking at it from the segment of spoofing the information exchange of the enemy, there are three segments that are indispensable, which are to dupe the enemy battlefield reconnaissance equipment, systems, and personnel; to dupe the enemy intelligence departments; and to dupe the enemy commanders. The information campaign must be combined with the firepower campaigns and the military troop campaigns, and each of the directions, each of the spaces, and each of the phases of the campaign must also be combined, so that they are capable of duping the enemy personnel, to the maximum extent possible. The third is that the information campaign must be combined with the information defense. Whether or not the information campaign is successful, to a certain degree, determines the information security protection results of the Chinese. Furthermore, concealing the Chinese information systems is also one of the pieces of content of the information campaigns. Therefore, during the implementation of the information campaigns, they must adopt strict confidentiality and security measures to strengthen the information defense, in order to guarantee the campaign results.

IV. Information pollution methods…112

Information pollution methods refers to the information attack fighting methods that **[end of page 112]** obstruct and infringe on the enemy information transmission channels, through the intentional overload of false, useless, and malicious information at the enemy, which destroys the corresponding information that the enemy uses, and pollutes the operational environment of the enemy information systems, in order to achieve the effects of restricting the normal command of the enemy information systems. This fighting method mainly implements attacks against the enemy information network systems, and through the wired or wireless channels, it infiltrates the internal enemy networks, so they can issue false information, and send out or launch the hacker procedures and viruses, to reduce the efficiency of the enemy network communications, and destroy the use of complete, accurate, and useful information on the enemy networks, which finally causes the enemy to not be able to normally use the information systems, which decreases the overall combat of the enemy and their command capabilities.

With regard to the use of the information pollution methods, first of all, they should implement information obstruction. Though the large amount of false information and useless information that is disseminated against the enemy information systems, it creates an "information torrent," which obstructs and infringes upon the enemy information transmissions channels, which causes the enemy information systems to be saturated and overloaded. This destroys the prompt collection, transmission, and processing of all of the essential enemy information, which ultimately cripples and even paralyzes the information systems. The second is that they should implement destruction through the use of viruses. The use of wireless viruses to empty into the technology equipment uses different types of viruses to get into the enemy information networks, infecting the enemy network information centers, as well as their important nodes and terminals, and then, through the remote issuing of orders, it activates the launch of the virus, which implements destruction of the enemy information networks, deletes and revises its data and leads to the enemy systems killing the computer and collapsing it. The third is that it implements external pollution. Using all types of gas heating and cooling systems and fog and smoke equipment, they can use all types of methods to combine native and foreign methods, to confuse the enemy information reconnaissance systems, and through the transmission of all kinds of useless or harmful information onto the enemy information channels or information sources, it influences and reduces the operational effectiveness of the enemy information systems and weakens the enemy information operations capabilities.

V. Information paralysis methods…113

The information paralysis methods are the integrated use of electronic interference, physical destruction, and other hardware and software methods, to separately implement attacks against the enemy information reconnaissance subsystems, information transmission subsystems, and information processing subsystems, to sever their mutual connections and destroy the integrity of the enemy information systems,

causing them to have difficulty in effectively bringing out their functions. This is mainly through the destruction of nodes to achieve the objective of paralyzing **[end of page 113]** the systems. Specifically speaking, it concentrates the military forces and military weapons of the information attacks and determines the strategic position of the function (nodes) against the enemy information systems, in order to implement electronic interference, virus attacks, and firepower destruction, in order to reduce or destroy the overall combat effectiveness of the enemy information systems. These nodes refer to the strategic positions and crucial points that determine the function for these entire information systems. This normally includes the command and control modules of the information systems, the communications exchange centers, such as the command centers of the information systems, as well as each of the centers of the subsystems, the early warning command organizations of the airspace above the battlefield, the main trunk line nodes of the regional communications systems, the command post communications centers of the command networks, the intelligence reporting stations of the radar networks, etc.

With regard to using the information paralysis methods, the first is that on the basis of implementing reconnaissance and analysis on the enemy information systems, they must accurately select and determine the key nodes. Using the mobile subscriber equipment (MSE) of the United States military, in the areas of military and commanders as the example, the coverage area of this system can reach 150 x 250 square kilometers, it is comprised of 42 central nodes, and it uses wireless radio relay equipment to connect the nodes. If these nodes happen to be destroyed, the information systems can be easily bogged down and paralyzed, and they cannot be used normally. The second is that during the implementation of the attacks on the nodes, they must assemble the military forces, integrate the use of all types of information combat forces, use a combination of the electronics attacks and network attacks, combine conventional combat and specialized combat, combine the soft kill and hard destruction, in order to swiftly and violently gain dominance, break through the enemy information defense, and implement a strong degree of damages on the important objectives, causing a period that is hard to recover from, thereby guaranteeing the attack results.

Section 3: Joint Campaign Information Fighting Methods…114

Information defense refers to the information system protection as well as the information security measures and activities that are combined with the information attacks, in order to protect the security of the information and information systems of the Chinese, based on the unified plan of the joint campaign commanders as well as their information combat commanding organizations, and it guarantees **[end of page 114]** the collection, transmission, and processing, and application capabilities of the information. Furthermore, it is the content that has been adopted that regards the anti-reconnaissance, anti-interference, anti-destruction, and anti-computer attacks as the important content. The main tasks of the information defense include three aspects, the protection of the information system security, the information security confidentiality, and the psychological defense. The protection of the information systems security is mainly done

through the anti-reconnaissance, anti-destruction, anti-attacks, and other methods, which are used to protect the normal operations of the Chinese systems. The information security confidentiality is mainly done through the information encryption, information concealing, identity discrimination, and other methods, which protect against enemy eavesdropping, protect against the enemy cracking the code, and protect against distortion, which protect the security of the Chinese combat information, its integrity, and its use. The psychological defense is mainly the use of communications, broadcasts, television, networks, and other modern communications media, to one, use the principles of psychology to enhance the spread of education of patriotism, to stimulate and encourage the military and the people to participate in the supportive feelings of the war, and to establish a firm belief that they will not fail; furthermore, it exposes the scattered falsities and erroneous information, that they are facing from the enemy's psychological warfare operations that they could adopt, through the technological measures that can destroy the psychological battle, in order to achieve the objectives of the morale of the soldiers.

The fundamental fighting methods of information defense are: information concealing methods, information deception methods, information central network methods, and information protective screen methods.

I. Information concealing methods…115

Information concealing methods refers to the type of information defense methods that use integrated radiation control, signal concealing, and other measures, to conceal the major electronic information systems of the Chinese, to the maximum degree possible, as well as their true information of the radiation, in order to prevent or reduce the enemy from effective electronics reconnaissance and anti-radiation destruction. Regardless of whether it is before the war or during the war, information concealing is the most fundamental method of information defense.

With regard to the use of information concealing methods, number one, they must control the information. The control of the information refers to the probability of reducing the enemy interception of our electromagnetic information, under a unified plan, in order to complete the most restricted prerequisite conditions of all of the required tasks, through the control of our radiation times and radiation scopes of our information system electromagnetic capabilities **[end of page 115]**. The control of the radiation times refers to the probability of reducing the exposed time that the electromagnetic waves are in the air, and reducing the opportunities for the Chinese information to be scouted or intercepted by the enemy, thereby decreasing the Chinese information from being destroyed by the enemy's anti-radiation methods, electronic interference, network attacks, and firepower attacks. The specific methods are to strictly control the direction and degree of electromagnetic radiation, to strictly control the amount and time of the information transmission, to simplify the electronic documents, to condense the connection times, and furthermore, they should implement effective electronic interference against the enemy electronics reconnaissance equipment, and reduce the

reconnaissance effectiveness of the enemy. The scope of the radiation control is to control the radiation direction and distance of the system electromagnetic waves, and to create as large of a reconnaissance blind area as possible for the enemy. Radio systems, under the prerequisite of guaranteeing the completion of the tasks, must insist upon the power being small rather than big. The position of the accurate and reasonable deployment of the launch equipment, and the prevention of forming an excessive concentration of electronic launch points, uses the deployment of the reasonable optimization to enhance the information defense. Second of all, they must conceal the signal. The concealment of information is the increased concealment that is used to avoid the enemy's reconnaissance of our electromagnetic information and the corresponding characteristics of the electromagnetic spectrum and the information content. The specific methods include: the concealment of the spectrum, using spread spectrum communications, frequency hopping communications, burst communications, and other technology methods, in order to reduce the probability of the signal spectrum exposure; the concealment of the electronic documents, using encrypted technology in each segment of the communications; and the information characteristics of the concealed signal. With regard to using the concealed defense methods, they must be flexible to changes, and they must respond quickly. In the 1960s, the Chinese Air Force guided missile troops and the electronics of the high altitude Taiwanese reconnaissance aircraft under United States control during the war, created "close and quick fighting methods," which is the model for the flexible use of concealed defense methods. After the enemy aircraft used the electronic early warning systems to discover our ground to air guided missiles and guided radar electromagnetic waves, they mobilized and evaded. Our air defense troops formulated the "close and quick fighting methods," which were that the guided radar would suddenly open up their antennas (or increase the high pressure) at close distances, it would quickly seize the objective, quickly implement the anti-jamming measures, simplify the command procedures and the attack instructions, and quickly launch the guided missiles, which caused the aircraft of the invaders to not have enough time to mobilize, succeed in escaping, and implement effective electronics interference. The core of the "close and quick fighting methods" is the two words, "close" and "quick." "Close" is to conceal the electromagnetic radiation and combat intentions of the Chinese, and **[end of page 116]** "quick" is, under the situations of the concealed electromagnetic radiation, the essential selections for completing the combat tasks, or else they could hinder the military operations. The mobilization flexibility and rapid response ideology that are reflected in the "close and quick fighting methods" have a general guiding significance for the other information defense methods as well as the information fighting methods.

II. Information deception method…117

Information deception method refers to each of the types of technology and the war technology measures that are jointly used for information deception, which uses the combination of feigning activities, simulations, and posing activities, the integration of information source deception, information channel deception, and information content deception, as well as concealing the real and exposing the fake information, thereby

achieving the information defense methods for implementing concealment and camouflage of the Chinese information and information systems.

The information deception can be implemented through various types of methods. Based on the objectives and results of the deception, information deception can be divided into three types: concealment style deception, obscure style deception, and guided style deception. The main objective of concealment style deception is to obtain the source of the information through the analysis of the enemy of their methods to "conceal the truth" by concealing their information, thereby guaranteeing the real information source is not discovered. During the implementation of the concealment style deception, what is normally used is the strict technology feigning activities, especially the implementation of stealth technology and encryption and decreasing the information leaks to their lowest levels. The obscure style deception is mainly the information volume of each type of information, through the increase and authentication of information that does not conform or is fundamentally contrasting or contradictory, causing the enemy to waste large amounts of time and energy during their information collection, discrimination, transmission, and processing, so they are not able to face the various types of possibilities, making it hard to accept or reject it, making it hard to put forth effective and accurate analyses and assessments, and thereby making them do many types of preparations, scattering their forces, or causing them to finally distinguish the true information. It also causes them to put off the time for doing the assessments and for adopting the correct measures, thereby losing their initiative. The guided style deception makes the situations that are opposite of the actual information or the situations that do not comply have a high degree of "authenticity," through increasing the degree of clarity of the deceptive information, thereby causing the enemy to neglect the genuine information or make the genuine information the false situation, even treating it as the duped information, and ultimately making erroneous decisions. In the specific implementation **[end of page 117]**, they should combine the actual situations of the time to determine the types of deceptive measures that they should adopt.

With regard to using the information deception methods, one, they must direct it against different equipment and use corresponding feigning fighting methods. The information feigning is focused against the enemy's high resolution reconnaissance equipment and relatively strong firepower attack capabilities. On the foundation of having highly effective security configurations, they should use each type of feigning technology on the information systems to implement focused feigning, protecting it from enemy destruction, and decreasing the enemy information attack effectiveness. The exercises have proven that the feigning, even in highly technical battles, can still have a relatively good function. Therefore, we must focus on the feigning work of the information systems. With regard to the different electronics equipment, we must use corresponding feigning methods, and we must pay attention to the specific characteristics of the equipment, as well as to implementing the feigning as we please. With regard to the important objectives, they can use ground decoys, camouflage nets, metal angles of reflection, invisible paint, and other equipment to implement strict feigning. They can also use smoke screens, etc. to implement concealed feigning, in order to decrease the reconnaissance results of the enemy electrical equipment. Two is that they need to

combine disguising the truth and revealing the falsities. The disguise of the truth is to do the information feigning work well, causing the enemy personnel "to not see," and to "not be able to attack" the Chinese electronics equipment. Revealing the falsities is "to reveal false appearances to the enemy," namely through each type of deceptive measure, such as implementing radio feigning, using corner reflectors and false command posts and battle locations, etc. of the false equipment, mixing together the false and real, causing the enemy to erroneously see and erroneously attack, effectively adjusting the enemy information attack capabilities, and shielding the normal use of the Chinese electronics information systems. "Revealing the truth" is intentionally revealing a few of the important Chinese electronics objectives to the enemy, in order to attract their implementation of reconnaissance and jamming, to reach the objectives for protecting the overall information systems. During the Kosovo War, the NATO military forces used methods such as iron underneath the areas where bonfires were set, old gun barrels filled with boiling water, and hanging corner reflectors on both sides of the highways, etc. Within the surrounding regions of the actual goals, they simulated each type of signal source, they disguised them into various fake objectives, such as tanks, cannons, guided missile sites, etc., and successfully deceived the NATO reconnaissance, wasting much of the ammunition of the enemy, and also protecting against their own actual objectives from being attacked. Furthermore, the radar, guided missile troops, armored forces, and mechanized forces, on the foundation of good disguises, often modified their configuration **[end of page 118]**, causing NATO to find it very difficult to scout the accurate positions, thereby having no way to implement the attacks. The third is that the information sources, information channels, and intelligence deception should be combined. The information source deception is the establishment of false information radiation sources, which attract the enemy electromagnetic information reconnaissance and attack forces and equipment. When the enemy is distinguishing our information sources from the false targets, we can change the false to be the true, using the "false launch source" to transmit the electromagnetic signal. The information channel deception is, during the electromagnetic information transmission process, based on the requirement for agreeing on the frequent transmission of information transmission channels, the coexistence of both the true and false information channels, which increases the degree of difficulty for the enemy reconnaissance. The intelligence deception is the use of all types of measures, especially the use of the information intelligence analysis systems that regard the permitted operations and the command controls as the priority, which cleverly carries out the schemes, and deceives the intelligence collecting and processing analysis systems of the enemy.

III. Information network method…119

The information network method refers to the information defense methods that fully use multiple types of electronic information equipment and systems to adopt different organizational formats and methods, based on the netted shape structure for the implementation of the configuration of the equipment on the information systems, during the campaign fighting, to optimize the structure, to guarantee that things are confused, that some things are blind and some are clear, some are suspended, and some go through,

in order for the systems to completely be capable of effective anti-interference, anti-destruction, and anti-stealth.

With regard to the use of the information network methods, the first is that in the aspects of the communications electronics defense, they can use the radio platforms, radio relays, and every type of wired communications method structure, to freely connect to and link to circuitous netted shaped systems, through the optimization of the system structures and configurations, to increase the electronics defense capabilities of the systems. Within a certain scope, they can also combine the communications networks, duplex radio mobile communications networks, single radio communications networks, tactical satellite communications networks, scattered communications networks, etc., to form an integrated field communications system with a combination of all types of network structures and formats, so they can increase the integrated communications support capabilities, and so they can also improve the information defense levels of the system, from a fundamental standpoint. The second is that with regard to the radar electronics defense aspects, the structure has "four defense" functions for the area radar network air defense system, which jointly uses the typical examples of the network defense methods. During modern combat, the use of the air defense radars faces **[end of page 119]** the threats of four types of advanced electronics combat, reconnaissance interference, anti-radiation weapon attacks, stealth aircraft attacks, and guided missile attacks. With regard to a single radar station or radar system, with regard to the improvement of a single type technology, it is very difficult to effectively counter the four types of threats that can simultaneously exist on the modern battlefield. They can use each type of different radar structure, based on the reasonable structural deployment, to make one radar technology system, and under the unified command, they can form an area radar network air defense system that has the "four defense" functions. They can implement system warfare with the enemy, and they can fully bring out the limited technology equipment functions of the Chinese military. During the optimization of the system structure, they can gradually integrate the new technology into the systems, making the old equipment newer, and effectively countering the sudden emergence of new threats. During the Second World War, the British established a radar network that was comprised of twenty different radar stations, which obtained the amount and courses of the German aircraft, and other information, in advance, which accomplished a great achievement for combating the German air raids.

IV. Information screen method…120

The information screen method is a type of information defense method that jointly uses sourced and passive electronics interference and other measures, against the enemy implementation of interference with electronics reconnaissance systems in specially designated directions and regions, and using specialized networks, specialized protocols, and other methods, to physically or logically isolate the connection between important information systems and external systems, as well as weaken the electronic reconnaissance and network reconnaissance capabilities of the enemy against our important directions or regions.

With regard to using the information screen method, the first is that they must implement fixed direction electromagnetic screens. The fixed direction electromagnetic screens are mainly used in the forward position of the Chinese military electronic information systems. Using the throwing style or display style interference equipment, it uses the radiation direction of the electromagnetic interference aimed at the reconnaissance stations in the direction of the enemy, and it implements obstruction style or aimed style interference against the enemy. Under the prerequisite of not affecting our own communications, it causes the enemy to not be able to scout our own communications and the communications between us and the enemy, and it establishes an intangible fixed direction electromagnetic screen. The second is that it implements regional electromagnetic screens. The regional electromagnetic screens are directed against the many reconnaissance stations that the enemy has deployed within the campaign and battle areas, which causes them to implement close interference on the throwing type jammers being used, or implementing airborne interference against the enemy unmanned aircraft that the enemy has used to get into the airspace of the battlefield **[end of page 120]**. They must form a specific standardized regional electromagnetic screen. They can also use the aircraft and vessels between the enemy radar, communications reconnaissance, and photoelectricity probe equipment and our information systems, to deploy a certain thickness and surface area of chaff, gas sol, smoke shell bomb, and other passive interference sources, in order to weaken the survey capabilities of the enemy radar and photoelectric equipment on our operational goals. The fixed electromagnetic screen and regional screens prevent the enemy implementation of the interference anti-reconnaissance functions and the implementation of the reconnaissance against our communications centers and information networks, and their common characteristics are to attack in order to assist in the prevention. Furthermore, they must pay attention to the implementation under unified commands, and they cannot, during the interference of the enemy, affect the normal communications of the Chinese military. They must also do the interference analysis work well, and promptly achieve the feedback of information of the interference results, in order to make progress in improving the preparation conditions for the interference methods or interference styles. The third is that they must implement specialized network isolations. The specialized network isolations refer to the use of individual physical specialized networks or logical simulated networks, to promptly use the specialized network protocols and other methods, starting from severing the levels of the relationship of the foundational networks and the other networks, and actively preventing the outside personnel from looking into or damaging the networks. The communications systems, command and control systems, guided missile location systems, etc. of the Soviet military mainly used this type of technology and methodology, and due to the foundational core of the information systems being open, it increased the anti-reconnaissance and attack capabilities. In future joint campaigns, the Chinese military should also, on the foundation of guaranteeing the necessary connection of the joint commands, clearly define the corresponding specialized network boundaries and they must use effective network isolation measures, in order to increase the overall security and protection levels. **[end of page 121, end of chapter]**

Chapter 7
Joint Campaign Information Operations Command System of Systems [SoS] {*zhihui tixi*}…122

Studying the establishment of a joint campaign information operations (IO) command system {*zhihui tizhi*}, straightening out the command relationships {*zhuhui guanxi*} of the IO strengths {*liliang*} of all services and arms {*junbingzhong*}, and forming an IO integrated-whole composite strength {*zhengti heli*} are the issues which must first need resolution in implementing joint campaign IO command.

Section 1: The Necessity of Establishing a Joint Campaign IO Command SoS…122

The joint campaign IO command SoS signifies an integrated whole {*zhengti*} composed of a joint campaign's various IO command institutions {*zhihui jigou*}, according to certain relationships and functions {*zhineng*}. A rational joint campaign IO command SoS has important significance for ensuring the high efficiency {*gaoxiao*} and stability of joint campaign IO command.

I. Needs and requirements {*xuyao*} for realizing the joint campaign operational intent {*zuozhan yitu*}…122

In joint campaign operations under informationized {*xinxihua*} conditions, whether [we] can seize and maintain air dominance/supremacy {*zhikongquan*}, sea dominance {*zhihaiquan*}, and dominance {*kongzhiquan*} of the battlefield, and thus ultimately gain success in joint campaign operations, first of all is dependent on whether [we] can seize information dominance {*zhixinxiquan*}. To this end, within joint campaign operational command {*zuozhan zhihui*}, [we] must strengthen IO command. By establishing a joint campaign **[end of page 122]** IO command SoS, [we] enable commanders {*zhihuiyuan*} to tightly center on the general intention {*zong qitu*} of the joint campaign operations, thoroughly organize the IO attack and defense activities {*gongfang xingdong*}, to the maximum extent convert the latent ability {*qianneng*} of omni-service and arm {*zhu junbingzhong*} IO into actual capability for IO, and thus employ effective IO activities to ensure the realization of the joint campaign intent.

II. The basis for smoothly implementing IO…123

The joint campaign IO strength composition {*liliang goucheng*} is complex, and the mission types {*renwu leixing*} are diversified, so if the command relationships cannot be straightened out, that could bring about the phenomenon of chaos {*wuxu*} in operational activities {*zuozhan xingdong*}. Hence, only by placing the IO strengths of all services and arms under unified command and control [C2] {*tongyide zhihui kongzhi*}, according to the requirements {*yaoqiu*} of joint campaign command, can [commanders] tightly center on realizing the general objectives {*zongti mubiao*} of joint campaign IO, and implement the individual IO activities [of these strengths].

III. Prerequisites {*qianti*} for bringing into play the integrated-whole effectiveness {*zhengti xiaoneng*} of the IO strengths…123

The joint campaign IO means are diversified, its strengths complex, and its degree of difficulty in coordination {*xietong*} high. Only by establishing a joint campaign IO command SoS, to implement centralized unified command {*jizhong tongyi zhihui*} of IO, can [commanders] synthetically [comprehensively] apply {*zonghe yunyong*} multiple IO means, fully bring into play the respective strong points of multiple IO strengths, adjust-coordinate {*xietiao*} them consistently, and closely complement {*miqie peihe*} them, to form an integrated-whole composite strength for IO, and bring into play the maximum operational effectiveness {*zuozhan xiaoneng*}.

IV. Objective requirements for the development of a joint campaign command system {*tizhi*}…123

The requirements for a joint campaign operational command system are as follows: rationalness of the command division of labor {*zhihui fengong*}, clarity of the command authority limits {*zhihui quanxian*}, flexibility of command modes {*zhihui fangshi linghuo*}, and optimality of command effects {*zhihui xiaoguo zuiyou*}. These requirements, when organizing and implementing joint campaign IO, mandate the establishment of the corresponding command institutions, to strengthen the command of IO and to fully bring into play the effectiveness of IO. This is because of the following: first is that the main duty {*zhize*} of the joint campaign commander [JCC] {*lianhe zhanyi zhihuiyuan*} is to command {*tongling*} the joint campaign's overall situation {*quanju*}, so he can only carry out macroscopic command {*hongguan zhihui*} of the IO activity {*huodong*}. The specific command {*juti zhihui*} work of IO can only be assumed by the corresponding IO command institutions. Second is that IO is an operational activity jointly conducted by professional IO-issues strengths {*zhuanye xinxi zuozhan wenti liliang*} and nonprofessional IO strengths. **[end of page 123]** The requirements on their command are stringent, and thus require having specialized command institutions to implement command per their functions {*zhineng*} and principles. For example, within information offense {*xinxi jingong*}, [commanders] must, by organizing and using the various information offensive strengths, restrict the bringing into play of the effectiveness of the enemy information systems {*xinxi xitong*}; and within information defense {*xinxi fangyu*}, [they] must, by organizing and adjusting-coordinating the various information support strengths {*xinxi baozhang liliang*}, weaken the degree of harm from the enemy's information attacks.[9] This special quality {*teshuxing*} of command activity {*zhihui huodong*} has determined the objective quality {*keguanxing*} in establishing a joint campaign IO command SoS. Third is that following on the increasing prominence of the

[9] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

position and role {*diwei he zuoyong*} of the IO developing on the basis of electronic warfare [EW] {*dianzizhan*}, it is fully necessary to explore {*tansuo*} the problems of joining the tracks {接轨 *jiegui*} between a joint campaign IO command SoS and the joint campaign command system {*tizhi*}.

Section 2: The Basic Principles Which Should Be Followed in Establishing a Joint Campaign IO Command SoS…124

The joint campaign IO command SoS is a component {*zucheng bufen*} of our military's joint campaign operational command SoS {*tixi*}, and is an organic integrated whole of many levels {*cengci*} and many systems {*xitong*}. The establishing of a joint campaign IO command SoS should be mutually adapted to our military's joint campaign operational command SoS, and mutually adapted to our military's IO weapons and equipment levels {*wuqi zhuangbei shuiping*} and operational task organization {*zuozhan biancheng*} – to accomplish consistency of responsibilities/duties and authority {*zequan*}, being elite and highly efficient {*jinggan gaoxiao*}, and smoothness in relationships, to ensure the agility and high efficiency {*lingmin gaoxiao*} and stability and reliability of IO command. Concretely speaking, [command personnel] should follow the following several principles:

I. The principle of being affected [driven] by needs {*xuqiu qiandong*}…124

Being affected by needs means establishing the joint campaign IO command SoS based on the actual needs and requirements of IO. The needs of the joint campaign IO SoS are embodied in two respects. First is focusing on the integrated-whole quality {*zhengtixing*} of the joint campaign, and establishing a SoS which fully complements {*peitao*} the joint campaign command SoS. The establishment of the joint campaign IO SoS must be subordinate to and in the service of the needs and requirements of joint campaign operations. Second is focusing on the special quality of IO, **[end of page 124]** and establishing an IO command SoS mutually consistent with IO command needs. IO command has the characteristics {*tedian*} of a broad distribution of the objects of command {*zhihui duixiang*}, stringent requirements on command time limits, and diversification of command modes. Its command activity per se already has exceeded the scope of the traditional joint campaign battlefield, the time limits of the command process must be those of near-real time or rapid reaction, and the command modes are assuming the features {*tezheng*} of multiple avenues and diversification. Hence, only when the joint campaign IO command SoS has been adapted to these characteristics of IO command can it meet the needs and requirements of IO command.

II. The principle of consistency in responsibilities/duties and authority…125

The hierarchical setup {*cengci shezhi*} of the joint campaign IO command institutions must be rational, and the responsibilities assumed by the institutions at all levels must be consistent with the authority {权力 *quanli*} they possess. Either too many

or too few levels could break the balanced status {*zhuangtai*} of consistent responsibilities/duties and authority, and does not benefit high-efficiency, adjusted-coordinated C2 {*zhihui yu kongzhi*}. The operational procedures {*yunzuo chengxu*} for joint campaign IO command relationships must be clear-cut, and the command relationships among all essential factors {*yaosu*} must be adjusted-coordinated consistently, to avoid the phenomena of institutional overlap and multi-headed command, leading to the IO strengths not knowing what course to take {无所适从 *wusuo shicong*}.

III. The principle of being elite and highly efficient…125

The wide-ranging application of command automation means {*zidonghua zhihui shouduan*} has caused reductions in the scale of joint campaign command institutions and boosts in effectiveness, and the establishment of IO command institutions also should involve an elite [quality] and high efficiency. This is because of the following: first is that digitized information display facilities equipment {*shuzihua xinxi xianshi shebei*} has realized real-time display of the IO situation and of the battlefield information environment. Second is that the establishment of advanced IO command computer-aided decision-making databases {*fuzhu juece shujuku*} enables large savings on human labor and manual work {*shougong zuoye*}. Third is that advanced information transmission facilities equipment has provided reliable information transmission assisting support {*zhiyuan*} for IO command activity. Hence, the joint campaign IO command institutions can reduce the organized and allocated {*bianpei*} numbers of staff officers {*canmou*} and support personnel, to meet the requirement for being elite and highly efficient.

IV. The principle of subordination to the integrated whole…125

First, the joint campaign IO command system {*tizhi*} also is an important component of the joint campaign command system {*tizhi*}. **[end of page 125]** In terms relative to the joint campaign command system, the IO command system is a part; and it is present within the integrated whole of our military's joint campaign command system. The establishing of a scientific and rational IO command SoS must be subordinate to and in the service of the joint campaign command system. Next, joint campaign IO is part of the entirety of joint campaign operations, and its ultimate goal is to realize the joint campaign's general objectives. This then requires that IO activities must be subordinate to and comply with the needs and requirements of the integrated whole of joint campaign operations. Finally, the bringing into play of the operational integrated-whole strength to a very great extent is dependent on the tight combination {*jinmi jiehe*} of IO activities and other operational activities, as well as on the consistent adjusting-coordination among the two main bodies, attack and defense, of IO. In other words, it is dependent on a high degree of centralization and unification in command. But in order to realize centralized unified command, [commanders] must give full assurance in terms of the command system {*tizhi*}. Hence, when establishing the joint campaign IO command SoS, they must properly handle the relationship between the integrated whole and the part. In all respects, the command institution setup, the specification of duties and authority limits,

and the establishment of command relationships. [this SoS] must be subordinate to this integrated whole of our military's joint campaign command system.

V. The principle of technical restrictions…126

The joint campaign IO command SoS has direct and necessary ties to the IO weapons and equipment technical levels and to the information warfare [IW] task organization {*xinxizhan biancheng*}. From the macroscopic viewpoint, the IO weapons and equipment technical levels determine the structure and types of the IO command system; this is the specific embodiment of this law of war {*zhanzheng guilyu*}, that military technology determines the armed forces system and organizational structure {*jundui tizhi bianzhi*} and strategy and tactics {*zhanlue zhanshu*}, within the IO command system. From the microscopic {*weiguan*} viewpoint, the specific task organization of the IO strengths determines the specific structure of the command SoS. From the viewpoint of the trend of development, following on the boosts in the armed forces' informationized levels and the large-quantity employment of IO weapons, on the future digitized battlefield, battlefield information networks will be linked into an organic whole {*yiti*} up to the supreme command authority {*zuigao zhihui dangju*} and down to individuals {*danbing*}, and will inevitably make the command system develop in the direction of network integration {*wangluo yitihua*}. This type of integrated operational command system will enable commanders to directly command the subordinate operational units at any level, and even directly command individuals. Hence, only when the joint campaign **[end of page 126]** IO command SoS is mutually adapted to the IO weapons and equipment technical levels and unit task organization can the entire command system smoothly operate {*yunxing*}. Otherwise, it could cause command loss of control {*shikong*} or low efficiency of command.

Section 3: Establishment of the Joint Campaign IO Command SoS…127

Establishing an IO command *tixi* system suited for IO command within a joint campaign ensures the implementation of effective command towards IO activities, allows for forming an integrated whole for IO activities, and is an important prerequisite for closely complementing other operational activities. Consequently, in the preparations phase of joint campaign IO, after the joint campaign commander receives and accepts the campaign tasking {*renwu*}, the first job is to establish a IO command *tixi* system suited for joint campaign IO.

I. Command institutions…127

Within joint campaigns, the IO command institution is the JCC's staff team {*canmou banzi*} for employment of the IO strengths; it is an organic component of the entire joint campaign command institution; and it is the core institution for formulating campaign IO plans {*jihua*}, for adjusting-coordinating the IO strengths, for operations-research-based planning of IO activities, and for commanding the IO strengths within the task organization of the campaign {*zhanyi biancheng*}. Under the usual circumstances,

the IO command institution should be simultaneously established with the entire joint campaign command institution.

The establishment of the IO command institution usually has two forms {形式 *xingshi*}: first is the establishment of a tri-level command institution, i.e., a 3-level command institution composed of the joint campaign command's IO department {*lianhe zhanyi zhihuibu xinxi zuozhan bumen*}, the IO departments of the various services' and arms' operational group commands {*zuozhan jituan zhihuibu*}, and the IO unit command posts {*budui zhihui suo*} (see Figure 7.1). Second is establishment of a bi-level command institution. This is a 2-level command institution composed of the joint campaign command's IO department and the various services' and arms' IO unit **[end of page 127]** command posts (see Figure 7.2).

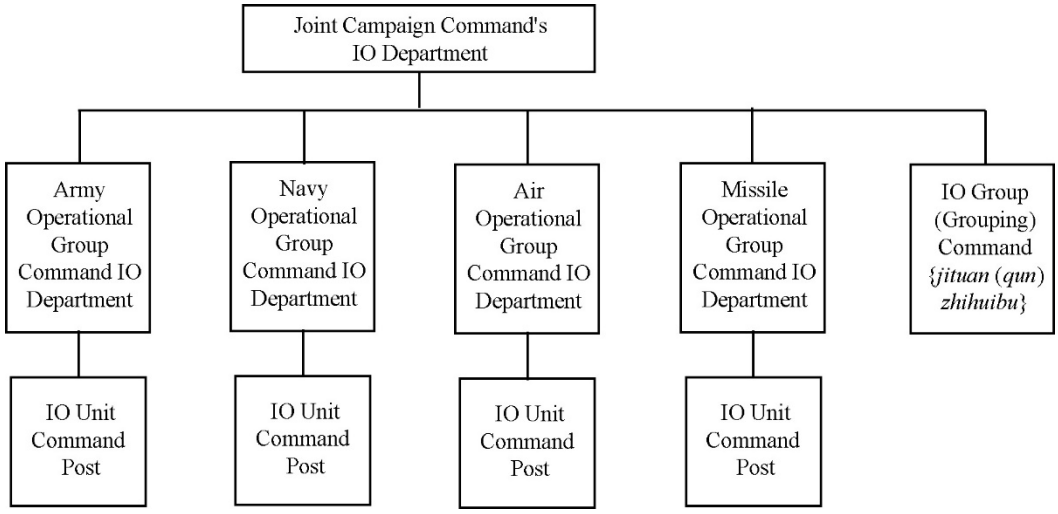

Figure 7.1: Schematic of Joint Campaign IO Tri-level Command SoS

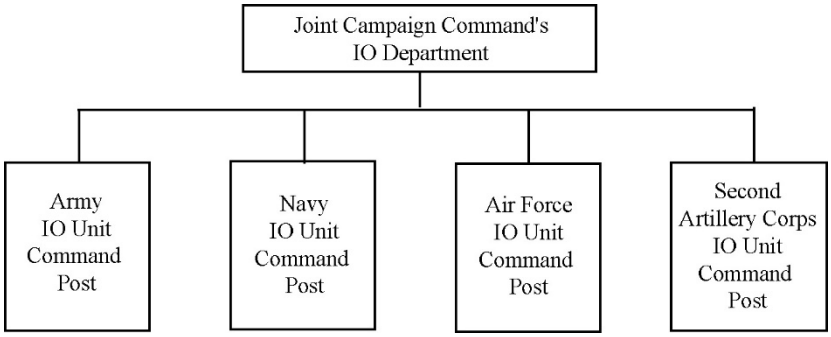

Figure 7.2: Schematic of Joint Campaign IO Bi-level Command SoS
[end of page 128]

The internal organizational grouping {*neibu bianzu*} of the joint campaign IO department can adopt different models {*moshi*}, mainly including the following two:

In the first model, the joint campaign IO department is composed of a comprehensive planning team {*zonghe jihua zu*}, IO reconnaissance team {*zhencha zu*}, information offense team, information defense team, and comprehensive support team. (See Figure 7.3.)

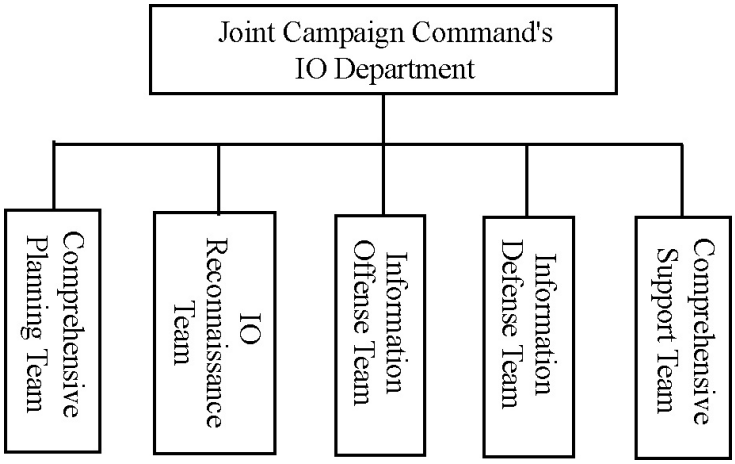

Fig. 7.3: One Schematic for Joint Campaign Command's IO Department Organizational Grouping

This construction model is one put forth on the basis of systems integration thought {*xitong jicheng sixiang*} for joint operations, and is a relatively ideal, fairly high-level construction model. In this type of construction model, the establishment of a comprehensive planning and adjusting-coordination team is in order to unify the work of adjusting-coordination among the IO center's various small teams {*xiaozu*}; to make it easy for the information offense, information defense, and information support activities to achieve consistent adjusting-coordination; and to be beneficial to realizing integrated command of IO. The establishment of the comprehensive support team is in order to unify the planning and organizing of IO support, and has reflected the characteristics of the high degree of reliance of IO on high-tech support. The establishment of the three professional teams {*zhuanye zu*}, the IO reconnaissance team, the information offense team, and the information defense team, adopts an organizational grouping method which classifies IO according to type, has centralized command by a specialized department {*guikou zhihui*}, employs systems integration, and has a high degree of jointness {*lianhe*}. **[end of page 129]** The IO reconnaissance team and information offense team concentrate in the same place all of the strengths for the IO reconnaissance and information offense missions undertaken by the various services and arms. They have unified operations-research-based planning and command, so that they are tightly connected, complement one another, and to the maximum extent bring into play integrated-whole capability {*zhengti nengli*}, to conduct integrated reconnaissance against enemy information systems, and to conduct IO activities such as destruction of enemy entities {*shiti*}, electronic attack {*dianzi jingong*}, psychological attack {*xinli jingong*}, computer network attack [CNA] {*jisuanji wangluo jingong*}, and special forces assault {*tezhong budui tuji*} on enemy IO systems. The information defense team will

unify the operations-research-based planning and command of all IO strengths to carry out information defense, including commanding resistance to the enemy's entity destruction, and implementation of IO activities such as electronic defense and protection {*dianzi fangyu yu fanghu*}, INFOSEC secrecy, psychological protection, and defense and protection of computers and their network systems.

The duties of the various positions {*buwei*} internal to the first type of organizational grouping model are as follows:

The comprehensive planning team is composed of staff personnel having intimate knowledge of Army, Navy, Air Force, and Second Artillery Corps IO. Its main duties are operations-research-based planning of IO activities, and drafting {*nizhi*} of unified IO plans; responsibility for reporting (to higher levels) and transmission {*shangbao yu chuanda*} of various types of messages {*wendian*} and plans; based on the joint campaign senior officer's {*shouzhang*} requirements and IO plans, the adjusting-coordination and control of the IO units' operational activities; and, based on needs and requirements, the adjusting-coordination of IO and other operational activities, as well as of information offense and information defense activities.

The IO reconnaissance team is composed of staff personnel having intimate knowledge of all services' and arms' EW reconnaissance {*dianzi duikang zhencha*} and computer network reconnaissance. Its duties are the formulation of IO reconnaissance plans, and the command and adjusting-coordination of the IO reconnaissance activities of all services and arms.

The information offense team is composed of staff personnel having intimate knowledge of all services' and arms' IO. Its main duties are formulation of information offense and information deception {*xinxi qipian*} activities plans, and command of the information offense activities of all services and arms.

The information defense team is composed of staff personnel having intimate knowledge of all services' and arms' communication [countermeasures] and EW {*tongxin, dianzi duikang*}. Its main duties are formulation of information defense plans for electronic counter-jamming {*dianzi fanganrao*} and electronic camouflage {*dianzi weizhuang*}, and for defending against enemy precision-guided munition [PGM] {*jingque zhidao wuqi*} attacks, and adjusting-coordinating and guiding all units within the operational task organization **[end of page 130]** in conducting information defense.

The comprehensive support team is composed of personnel from the communication, computer, command automation, and equipment technology departments of all services and arms. Its main duties are formulation of IO materiel {*wuzi*} and equipment technical support plans, adjusting-coordination and allocation and transfer {调拨 *diaobo*} of IO weapons and equipment and command automation and network facilities equipment, and adjusting-coordination of maintenance {*weixiu*} and support for all types of IO weapons and equipment.

In the second model, the joint campaign IO department is composed of a comprehensive planning team, entity destruction control team, EW {*dianzizhan*} team, network warfare {*wangluozhan*} team, INFOSEC support team, psychological warfare [PSYWAR] {*xinlizhan*} team, and comprehensive support team. (See Figure 7.4.)

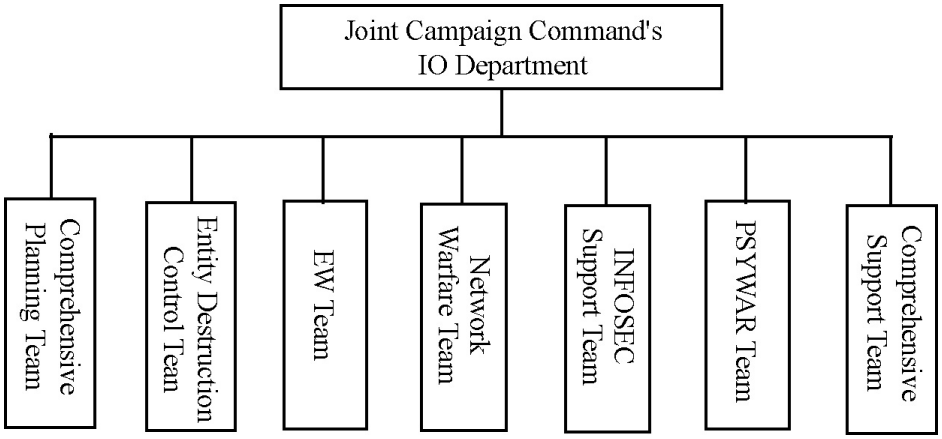

Fig. 7.4: Second Schematic, Joint Campaign Command's IO Department Organizational Grouping

This model is one established based on our military's existing IO strengths. Besides the comprehensive planning and adjusting-coordination team and the comprehensive support team, whose roles are the same as in the first model, its organization includes an entity destruction control team, EW team, and PSYWAR team, all of which already have a command organization within the existing command institutions. Some of them, even though {*jinguan*} they currently still lack clear-cut centralized organization in a special department {*guikou zuzhi*}, nonetheless there still are other command organizations which act on their behalf {*daixing*} to perform their duties. This is beneficial to rapidly establishing an IO center and rapidly forming command capability. This model also adds an INFOSEC **[end of page 131]** support team and network warfare team, whose aim is to lay stress on the position and role of IO activities such as computer network warfare [CNW] and INFOSEC secrecy within modern IO. This construction model has a fairly clear-cut division of labor, makes it easy to perform command duties, and is relatively suited to the reality of our military's present IO command and practice still being in an initial phase.

The main duties of the various positions internal to the second organizational grouping are as follows:

The duties of the comprehensive planning team and comprehensive support team are the same as in the organizational grouping in the first model.

The entity destruction control team is composed of personnel having intimate knowledge of the operations of the Second Artillery Corps, naval bombing aviation

forces {*haijun hongzha hangkongbing*} and ground attack aviation forces {*qiangji hangkongbing*}, Army aviation forces {*lujun hangkongbing*}, and special forces, as well as operations with PGMs. Its main duties are drafting of operational plans for effecting hard destruction of enemy information systems and informationized weapons and equipment, and complementing the joint campaign command center in adjusting-coordinating the units (elements) {*bu (fen) dui*} undertaking the hard-destruction missions in carrying out entity destruction operations

The EW team is composed of staff personnel having intimate knowledge of the EW strengths and employment requirements of the various services and arms, including those of the Army, Navy, Air Force, and Second Artillery Corps. Its main duties are collection and processing of EW intelligence; putting forth EW resolution recommendations {*juexin jianyi*}; drafting of EW operational plans; transmission of EW operational orders and instructions {*zhishi*}; organization of EW coordination and its various types of support; supervising-promoting {*ducu*}, inspection {*jiancha*} and reporting (to higher levels) of the operational preparations and implementation situation for campaign EW; and timely handling of problems arising during the EW implementation process.

The network warfare team is composed of related staff officers and technical personnel having intimate knowledge of communication, command automation, and computer networks. Its main duties are drafting of networking plans {*zuwang jihua*} for battlefield information transmission systems and command systems, and of information support plans; drafting of defense plans for computer systems, battlefield information network systems, and command information systems; guiding and adjusting-coordinating the IO strengths in conducting network operations; and carrying out maintenance {*weihu*} of informationized battlefield network systems.

The INFOSEC support team is composed of staff personnel for technical security secrecy {*jishu anquan baomi*}, communication, and cryptography {*jiyao*}. Its main duties are drafting of INFOSEC support plans, transmission of INFOSEC **[end of page 132]** support instructions and taking responsibility for information secrecy work, and, in a unified manner, carrying out battlefield EM spectrum management {*dianci pinpu guanzhi*} and cryptographic management {*mima guanli*}.

The PSYWAR team is composed of political work personnel and related personnel from PSYWAR units. Its main duties are unified drafting of PSYWAR plans, including those for wartime news control {*xinwen guanzhi*}, and of operational activities plans with psychological deterrence {*xinli weishe*} as the goal, and guidance of the units' PSYWAR activities.

Within specific operations, the model which the IO department finally adopts should be determined based on our military's operational training levels {*zuozhan xunlian shuiping*}, the degree of development of information weapons and equipment, and the JCC's related instructions and requirements. However, no matter which model is

adopted, it always should clarify its basic missions and duties, and the personnel composition always should be scientific and rational.

II. Basic duties…133

The IO department, according to the JCC's resolution and intent, and under direct leadership by the head of the C2 center {指控中心 *zhikong zhongxin*}, performs the following duties: first is organizing of the joint campaign IO reconnaissance, and grasping of the IO-related situation. Second is putting forth of the joint campaign's IO reports and resolution recommendations. Third is organizing and drafting of IO plans. Fourth is receiving and execution of the higher-level IO orders and instructions, and briefing {*tongbao*} of the IO situation to the lower levels. Fifth is organizing and adjusting-coordinating the Army, Navy, Air Force, and Second Artillery Corps IO strengths within the task organization of campaign in conducting IO reconnaissance, information offense, and information defense against the enemy. Sixth is organizing of IO coordination and professional support. Seventh is supervising-promoting and inspection of the lower levels' preparations for IO. Eighth is commanding and adjusting-coordinating all IO activities, and timely analysis and resolution of problems arising during the IO implementation process. Ninth is fulfilling other correlated missions {*xiangguan renwu*} entrusted by the JCC.

The IO departments of the various services' and arms' campaign large formations {*zhanyi juntuan*}, within the scope of their corresponding responsibilities and authority, perform functions {*zhineng*} similar to those of the joint campaign command's {联指 *lianzhi*} IO department. What is different is that the IO department of the joint command's C2 center is responsible for IO command within the entire campaign scope, **[end of page 133]** and lays particular emphasis on integrated-whole working out an approach in planning {*zhengti mouhua*} and on the guiding and adjusting-coordination work. By contrast, the IO departments of the various services and arms center on the joint campaign IO missions, and lay particular emphasis on the specific command of the IO activities of their root services and arms.

III. Command relationships…134

The joint campaign's participating {*canzhan*} IO strengths are numerous, and their missions complex. The command relationships for IO should, according to the requirements for being clear-cut, direct, convenient, smooth, and highly efficient, and based on the realities of the campaign, determine the command relationships, the attached relationships {*peishu guanxi*}, the coordination and assisting support (safeguarding support) relationships {*xietong yu zhiyuan (baozhang) guanxi*}, and the guidance relationships. The joint campaign IO department, under the specific leadership by and intent of the chief of staff {*canmouzhang*} and the head of the C2 center, launches {*kaizhan*} the work, puts into effect unified organization and planning of IO activities, and guides the operational activities of the IO units (elements). The IO group (grouping)

command {*jituan (qun) zhihuibu*} directly commands the operational activities of the subordinate IO units (elements).

The command relationships include the command relationships composed by the joint campaign command over the IO groups (groupings), by the IO group (grouping) commands over the subordinate IO units, and by the service and arm operational group commands over the subordinate IO units.

The attached relationship signifies the relationship formed between two units {*danwei*} when the JCC, in order to strengthen the operational capability {*zuozhan nengli*} of the IO units, temporarily allocates and transfers {*linshi diaobo*} some force-strengths back to the use of the IO units. After such an attached relationship is established, the IO unit commanders and their command organs {*zhihui jiguan*} implement all-around command and support of the operational activities of the attached unit(s). After an attached unit fulfills the predetermined mission(s), it can per orders return to its organizational system {归建 *guijian*}, and the attached relationship is correspondingly dissolved.

The coordination and assisting support relationship. Coordination and assisting support relationships can be clarified among all operational groups (task groups {*jiqun*}), among the IO units of all operational groups (task groups), between the IO units of different operational groups (task groups), and among the internal [parts] of the IO units subordinate to all groups (task groups), based on the differences in the IO missions and operational activities. **[end of page 134]**

Guidance relationships: guidance relationships are composed by the joint campaign command's IO department over the IO departments of all operational group (task group) commands, and by the IO departments of all service and arm operational group commands over subordinate IO unit command posts.

Section 4: Several Issues Which Should Be Grasped in Establishing the Joint Campaign IO Command SoS…135

The establishing of a joint campaign IO command SoS not only is one of the needs and requirements for propelling IO building, but also is one of the needs and requirements for boosting the real combat capability for IO. Hence, [command personnel] must occupy the high ground of the times, combine [the needs and requirements] with reality, focus on development, and actively and reliably carry out [this task].

I. Changing concepts {*guannian*}, expanding new viewing fields for establishing the joint campaign IO command SoS…135

Establishing the joint campaign IO command SoS requires changing three concepts. First is changing the concept that the JCC takes on all {包揽 *baolan*} IO

command authority {*zhihui quan*}. Some viewpoints hold that joint campaign IO command authority should be directly held by the JCC, and there is no necessity for then establishing a joint campaign IO command institution. In reality, for the JCC to completely assume the IO command mission could lead to dispersal {*fensan*} of the JCC's energy, and to weakening of his command and of his capability for controlling {*jiayu*} the overall situation of the joint campaign. Second is changing the concept that IO command authority can be taken on {*daixing*} by the IO work [service] functional departments {*yewu zhineng bumen*}. Some viewpoints hold that the intelligence, communication, and EW {*dianzi duikang*} departments within the joint campaign command institution all have their respective objects of command within IO, and that IO command authority can be taken on by these work functional departments. However, in fact the main energies of these work departments will be focused on processing their respective work, **[end of page 135]** making it difficult for them to also give consideration to the overall situation of IO. If the various work functional departments are made to serve as the joint campaign IO command institution, that inevitably will decentralize the IO command authority limits, and thus lead to chaos in the IO activities. Third is changing the concept that the functions of a joint campaign IO command institution [can be] taken on by a certain work department. In reality, any one functional department within the IO command institution never has the authority {*quanwei*} for commanding IO. The exercise of IO command authority by a certain functional department clearly would violate the law of objective quality {*keguanxing*} in terms of the functional partitioning {*zhineng huafen*} of the joint campaign IO command institution, and is something which cannot be established. Hence, study of joint campaign IO command issues must further expand the viewing field.

II. Strengthening legislation, seeing that the establishment of the joint campaign IO command SoS moves onto the new track of advancement according to law {*yifa tuijin*}…136

At the present time, among important operational rules {*zuozhan fagui*}, such as the *Chinese People's Liberation Army [CPLA] Joint Campaign Guidelines* {*lianhe zhanyi gangyao*}, even though standards [norms] {*guifan*} have been laid out for establishing an IO department within a joint campaign command institution, nonetheless the position and role of the joint campaign IO command SoS within the joint campaign command SoS still have not been clarified, and issues such as the internal setup {*neibu shezhi*} and functional differentiation {*zhineng qufen*} of the joint campaign IO command institution have still not been standardized [normalized]. From the viewpoint of establishing needs for the joint campaign IO command SoS, there is a necessity when revising {*xiuding*} the related operational laws to correspondingly increase the content of IO command SoS building, and, via exercises {*yanxi*}, to test {*jianyan*} the different command modes and efficiencies {*xiaolyu*} of the professional and nonprofessional IO strengths; then to gradually elevate them to the level of the joint campaign; and finally to implement them within joint campaigns. By strengthening the legislation, [we] ensure that the establishment of the joint campaign IO command institution has laws to abide by {有法可依 *youfa keyi*} and has rules to follow {有章可循 *youzhang kexun*}.

III. Being bold in practice, exploring new laws for establishing the joint campaign IO command SoS…136

First is the need to carry out testing {*jianyan*} of the envisioned {*shexiang*} joint campaign IO command institution within joint campaign exercises. When organizing joint campaign exercises, [the commander] can, in a manner having a directed [focused] quality {*you zhenduixing di*}, **[end of page 136]** set up an IO command institution; allow all levels to discover problems by operation {*yunzuo*} of the IO command institution; and, via practice, explore measures for resolving the problems, and seek the optimal avenue for establishing the joint campaign IO command SoS. Second is that, within the practice of joint campaign IO command SoS building, [the commander] must focus on development; persevere in a mutual combination of theoretical research and experience in practice; constantly strengthen research on IO command theory; deepen the understanding of IO command laws; and perfect a theory SoS [body of theory] {*lilun tixi*} conforming to our military's reality, and complying with the IO command principles, command system {*tizhi*}, and command modes needed and required for future operations. Third is the need to go through practice to verify {*yanzheng*} and perfect the joint campaign IO theory, and to use scientific theory to guide practice in joint campaign IO command institution building, and to maintain a scientific quality {*kexuexing*} in the structure of the joint campaign information operations command system of systems. **[end of page 137; end of chapter]**

Chapter 8
Joint Campaign Information Operations Preparations…138

Information operations [IO] preparations are the series of organizing and leadership activities conducted in advance in order to implement IO by the joint campaign commander and his command organ in accordance with the joint campaign intention. For IO preparations, one should meticulously perform operations research-based planning and thoroughly organize it on the basis of the peacetime preparations and in accordance with higher level intent and the objective realities of both sides. IO preparations normally include: organize readiness grade transitions; establish the IO command institution and clarify command relationships; receive the tasks and set down the IO resolution; issue IO tasks; formulate the IO plan; organize IO coordination; organize IO support and wartime political work; organize IO unit unfolding; organize and implement imminent battle training and supervise operational preparations. During a joint campaign, IO preparations are an important component of the entirety of campaign preparations. Thoroughly and successfully accomplishing each item of preparations work in IO not only is an important responsibility of the joint campaign commander and his command organ, but it also a prerequisite and foundation for smoothly implementing IO activities.

Section 1: Organize Readiness Grade Transitions…138

Readiness grade transitions normally refer to transitioning from a daily readiness {*jingchangxing*} to a higher grade readiness or from a daily readiness grade by skipping grades directly to the necessary readiness grade. The joint **[end of page 138]** campaign command organ should, in accordance with higher level orders and instructions, issue readiness grade transition orders to participating IO units at the right time and strictly organize readiness grade transitions. Under the guidance of the joint campaign command headquarters {*zhihuibu*}, IO units should successfully accomplish the following work when organizing readiness grade transitions:

— Receive the joint command readiness grade transition order and instruction; combining it with the IO missions, relay the readiness grade transition orders; and issue the readiness grade transition advance order to subordinate units.

— Revise and improve the maneuver {*jidong*}, expansion of task-organization {*kuobian*}, air defense {*fangkong*} and operational {*zuozhan*} readiness courses of action {*zhanbei fang'an*}.

— Convene Party committee (operations) meeting; issue the higher level readiness grade transition order; and perform dispositioning of one's own level readiness grade transition work.

— Issue readiness grade transition order to the units. The readiness transition order contents mainly include: brief on the enemy situation; tasks that units are about to execute; readiness grade transition scale; the main work and time limits for completing readiness grade transitions; and requirements of each item of preparations work, etc. The readiness grade transition order should be prompt, brief and concise and secret, and it does not involve the higher level's general operational intention and the specific time of operational start. The time limit for completing readiness grade transition is normally stipulated correspondingly on the basis of the readiness grade and unit types.

— Organize readiness duty schedules {*zhanbei zhiban*}. This includes senior officer duty schedules, operations duty schedules and department duty schedules {*yewu bumen zhiban*}. Duty personnel should supervise-urge each IO unit to successfully accomplish each item of preparation work in accordance with different readiness requirements.

— Supervise-urge, inspect and guide unit readiness grade transitions. After the readiness transition order is issued, the IO commander and his command organ should conduct inspections, assistance and guidance for the mobilization preparation work situation of their subordinate units so as to ensure implementation of the readiness grade transition work. The main content of inspections are: understanding the higher level orders and instructions and execution situation; mobilization and thought education situations; repair and adjusting-replenishment [end of page 139] situation of weapons and equipment; and the implementation situation of each item of readiness zhidu system such as that of the readiness on-duty personnel.

— Higher level readiness grade transition situation. After accomplishing a readiness grade transition or on the basis of higher level requirements, one should promptly report up the readiness grade transition synthesized situation. The report contents mainly include: comprehension of higher level orders and instructions and their execution situation; readiness duty personnel situation; unit thought status and gathering of personnel situations; readiness courses of actions revisions and inspection-repair and adjustment of replenishment of weapons and equipment situations, etc.

— Readiness grade transition times are tight, contents are many and requirements are high, so the commander and his command organ should perform unified operations research-based planning, meticulously organize and ensure that readiness grade transitions are accomplished within the stipulated time limits.

Section 2: Receiving the Tasks, Setting the Information Operations Resolution…140

I. Receiving the tasks…140

The joint campaign commander, normally through a modes such as participating in an operational meeting or receiving higher level verbal or written operational order,

receives the IO tasks at the same time as receiving the general operational tasks. The joint campaign commander ordinarily does not singularly receive the IO tasks, but in a special situation, he may only receive the IO tasks.

The joint campaign commander, when he receives the IO tasks, should be clear on the higher level general operational intention, the higher level's IO intention as well as the issues he should pay attention to with key points in implementing that operational intention; the explicit IO tasks that higher level's have given to his level and the basic requirements for accomplishing the IO tasks; the IO tasks of the other directions and the effects of accomplishing the IO tasks at his level.

After the joint campaign commander receives the tasks, he should quickly relay it to the command organ the following: the enemy situation and higher level intent {*yitu*}; the IO tasks of their own level; **[end of page 140]** friendly situation; operational requirements and limiting conditions. After relaying the tasks, they should, on the basis of the total time for campaign preparations, scientifically plan and arrange each item of work in the campaign preparations phase, and instruct the IO departments to quickly formulate the work plan of the campaign preparations phase and prepare the relevant materials and IO synthesized resolution report recommendation {*zonghe juexin baogao jianyi*}; they should instruct the political work department, logistic support department and equipment support department to separately and quickly unfold their corresponding preparation work.

II. Setting the IO resolution…141

The IO resolution {*xinxi zuozhan juexin*} is the basic decision {*jueding*} accomplished by the joint campaign commander for IO activities; it is the basis for formulating the joint campaign IO plan, issuing IO orders and organizing IO coordination. During joint campaign operations, the IO resolution is an important component of the entire joint campaign resolution, so serving as a part of the campaign resolution is reflected in the entire campaign resolution. Setting the IO resolution is conducted on the basis of the sequence of comprehending the tasks; assessing the situations; determining the IO intention; dividing the tasks; clarifying the command, coordination and support items; listening to the reports and recommendations and determining the IO resolution.

(1) Comprehending the tasks

After receiving the IO tasks, the joint campaign commander should completely and accurately comprehend the tasks. This includes: comprehending the higher level intent, operational concept, main direction, operational disposition, differentiation of operational phases and the operational tasks of each phase; clarifying the relationships between IO activities and other operational activities; getting clear the nature of IO tasks, the goal and requirements to be reached and the position and role of IO in the overall situation of the campaign, etc.

(2) Assessing the situations

Assessing the battlefield IO situation is the prerequisite condition of setting the IO resolution. On the basis of fully understanding the IO tasks, the joint campaign commander should guide his relevant departments (such as IO, intelligence, communications, etc.), and on the basis of **[end of page 141]** completely analyzing and assessing the IO of both sides and the battlefield posture, set the correct IO resolution. Normally, the IO resolution an important content of the joint campaign commander's operational resolution and it is determined at the same time as the joint campaign commander sets the operational resolution. The IO resolution normally includes the following:

1. Enemy situation assessment

This mainly includes the following four areas:

The enemy's main commander's situation: mainly analyzing and assessing the situations such as the enemy commander's command characteristics and personality, the importance he attaches to information, information technology and IO application, and experience in implementing IO.

The enemy's information infrastructure and information systems: mainly analyzing and assessing the structure, distribution and necessary technical parameters of the enemy's information infrastructure; the critical information nodes or links in the information infrastructure; the degree of reliance on the information infrastructure; the locations of other infrastructure the information infrastructure must rely on; their capability to restore the important information infrastructure that is disrupted; their capability to handle the disruption of their information systems; the composition and deployment of the campaign command information system, especially the important parts such as the critical nodes.

The enemy's IO capability: mainly analyzing and assessing the enemy's IO intention; IO reconnaissance capability, information attack capability, information defense capability; the main direction for implementing IO, the IO strength task-organization and disposition; the means and patterns they may implement information attack against us; the modes and capabilities that international influence may have on the enemy conducting IO support {*zhiyuan*}.

The weak points of the enemy's information systems: mainly analyzing and assessing the weak links of the enemy's air defense anti-missiles, intelligence and reconnaissance, command and control, communication and satellite navigation systems, finding out approaches {*duice*} to utilize their weak points, and analyzing any supplemental disruptions that may result from implementing IO against the enemy. **[End of page 142]**

2. Our situation assessment

This mainly includes: the military-government quality, operational capability and degree of readiness of IO units within the joint campaign task-organization; IO reconnaissance capability, information attack capability, information defense capability, electromagnetic spectrum management and control capability; the capability of commanders at each level to organize command and coordination of IO.

3. Battlefield environment assessment

Mainly, ascertain the natural environment, social environment and electromagnetic environment of the operational area.

For the natural environment, this includes: the terrain characteristics of the operational area, in particular the effects of the direction of roads, valleys and mountain massifs and forest distribution on IO activities; the areas that are favorable for maneuvering and concealing the deployment of IO force strengths and weaponry; the flyby times, position fixes and operating orbits of various enemy reconnaissance satellites in the operations area; the distribution and operating situation of our command information systems in the operations area.

For the social environment, this includes: situations in the operations areas such as social, economic, cultural, ethnic religions and people's psychology; the support {*zhiyuan*} and support {*baozhang*} capabilities of local civilian information infrastructure on IO; the manpower and materials strength situation that the government can support {*zhiyuan*} IO.

For the electromagnetic environment, this includes: the situation of civilian electronic equipment distribution, television, radio and communication frequency spectrums and other electromagnetic emissions; the situations of the enemy's electronic interference equipment distribution and electronic jamming and the degree of influence on our operational activities.

4. Reaching a conclusion of the situation assessment

On the basis of analyzing and assessing the enemy situation, our situation and the battlefield situation, clarify the strong and weak points of the enemy information targets and the total capabilities of our IO operations as well as the degree of task completion.

(3) Determining the IO intention

The IO intention is the basic conceptualization made by the joint campaign commander on how to carry out IO on the basis of comprehending the tasks and assessing the situations, **[end of page 143]** and it is an important step in setting the IO

resolution. The content of the IO intention mainly includes: operational goal, operational targets, strength application, basic fighting methods, etc. After the IO intention is determined, quickly issue towards subordinates, and simultaneously clarify the times, sequence, content and methods for listening to reports and recommendations.

(4) Differentiating tasks, clarifying command, coordination and support items

Differentiating tasks is the task whereby the joint campaign commander preliminarily divides the IO units under his direct subordination and each service or arm. The joint campaign commander should, on the basis of earnestly understanding and grasping the operational capabilities of each participating IO unit and centering on the campaign intention, preliminarily determine the IO tasks of each service or arm operations group {*zuozhan jituan*} for the IO group {*jituan*} (grouping {*qun*}).

In clarifying command, coordination and support items, one mainly clarifies the following: the set-up location of the IO group's (grouping's) command post and the time for completing set-up and the time limit and requirements for establishing the information system[s]; IO coordination key points, coordination relationships and coordination forms and methods; the operational support, logistic support and equipment support key points of IO.

After differentiating tasks, and clarifying command, coordination and support items, one should promptly issue the operational advance order {*zuozhan yuxian haoling*} so as to allow the IO group (grouping) and the operations group IO units of each service or arm to conduct IO preparations as early as possible. The content of this is mainly: to preliminarily clarify the tasks, preparation work and completion time limit of the IO units of the IO group (grouping) or each service or arm as well as the items such as command, coordination and support.

(5) Listening to reports and recommendations

During the course of setting the IO resolution, one should listen to the IO reports and recommendations so as to allow the resolution to conform more to objective realities and to make the correct decision. Under ordinary situations, **[end of page 144]** one only listens to the synthesized report and recommendation put forth by his chief of staff; under special situations, one can separately listen to the reports and recommendations of his IO departments and IO unit commanders. Outside of this, depending on needs-requirements, one can consult relevant personnel of the IO departments at the appropriate times on the situations.

The IO reports and recommendations main contents include: situation assessment conclusions; the IO intention; the IO main direction and key point targets; the IO disposition; IO fighting methods; the times for completing operational preparations and initiating information attacks; and organizing of IO command.

(6) Determining the IO resolution

In determining the IO resolution, one normally should make the decision on the basis of correctly comprehending the IO tasks, completely understanding and grasping the enemy situation, our situation and battlefield situation, and listening to the IO situation reports and recommendations. The main contents include: IO intention; main operational direction and key point targets; IO disposition; fighting methods; times for completing IO preparations and initiating IO; and items of IO command and coordination.

1. Determining the IO goal

The IO goal is the anticipated outcome and goal to be reached in joint campaign IO. The joint campaign IO commander should correctly determine the Io goal based on the joint campaign intention, enemy situation, PLA IO capabilities, battlefield electromagnetic environment, etc. The IO goal can be implementing information attack and seizing and maintaining battlefield information dominance; [it can be] implementing information defense and ensuring our operational information security and a normal bringing into play of our information system effectiveness; [it can be] implementing IO reconnaissance and gathering the needed intelligence for joint campaign IO.

2. Determining the IO main direction and key point targets

The main direction of IO is the direction and areas/zones {*quyu*} for concentrating IO strengths and IO weaponry so as to implement the main information attack and seize information dominance against the enemy. **[End of page 145]** During a joint campaign, the main direction of IO in the majority of situations should be identical to the main direction of the campaign, but in different phases of the campaign, due to the specific goals of IO being different, the main direction of IO will change accordingly. One should select it on the basis of factors such as the joint campaign goal, main operational direction, the deployment of the enemy's information systems, etc. In determining the main direction of IO, one should be able to effectively support {*zhiyuan*} and support {*baozhang*} the operational activities in the main direction; and one should be able to effectively paralyze the enemy's information systems and destroy the important information targets.

The key point targets of IO are the enemy's important information targets that are selected with key points in order to seize (partial) information dominance. When determining key point targets of IO, one should select the critical nodes {*guanjian jiedian*} in the enemy's information systems having a significant effect on the operational activities of the various phases (time occasions). When determining the key point strike targets of IO, not only must one clarify specific directions and locations, but at the same time, one should successfully determine the priority sequence of strikes based on the degree of importance of the target and the possible course of the campaign.

3. Determining the IO fighting method

IO is normally divided into two basic types of information attack and information defense. The basic fighting methods of information attack are mainly: information deterrence {*xinxi weishe*}, information blockade {*xinxi fengsuo*}, information momentum creation {*xinxi zaoshi*}, information pollution {*xinxi wuran*}, and information paralysis {*xinxi tanhuan*}. The basic fighting methods of information defense are mainly: information concealment {*xinxi yinbi*}, information deception {*xinxi qipian*}, information network construction {信息组网 *xinxi zuwang*}, and information protective screening {信息屏障 *xinxi pingzhang*}. When determining the IO fighting methods, one should accomplish an organic adjusting-coordination {*youji xietiao*} with other operational fighting methods, and be mutually complementary so as to not only be beneficial for achieving the specific IO goal, but also create favorable conditions for other operational activities; one should, at the time-opportunity and place of employment, successfully determine the application of the IO fighting method from the perspective of the overall situation of the campaign, and not only must this be favorable for implementing effective strikes against the enemy, but it can also avoid as much as possible creating harmful effects for one's own activities.

4. Determining the IO disposition

The IO disposition is the strength task-organizational grouping, mission differentiation and deployment conducted for **[end of page 146]** various directly subordinate and attached IO strengths in accordance with the operational missions and fighting methods and on the basis of the unified plan. The joint campaign commander and his command organ should rationally determine the IO strength disposition on the basis of situations such as the joint campaign tasks, enemy situation, IO capabilities, battlefield environment, etc. In determining the IO disposition, one must: rationally employ the IO strengths, improve the degree of blending of various IO strengths, and form a stronger *tixi* system operational capability so as to benefit the bringing into play of the integrated-hole effectiveness of the IO strengths of various services and arms; in order to benefit the concentration of IO strengths in the main direction, areas and time occasions, [one must] form a localized information confrontation superiority against the enemy; and in order to support {*zhiyuan*} and complement the main campaign activities, [one must] adapt to the requirements of different operational patterns.

The form of task-organizationally grouping the IO strength is mainly determined according to the IO tasks, requirements and the specific situation at that time. When the joint campaign commander and his command organ are task-organizationally grouping the IO strength, they should abide by the shared requirements of task-organizationally grouping the IO strength, take aim at their specific situation of IO and implement a scientific, rational and flexible task-organizational grouping. There are normally two task-organizational grouping modes:

The first is whereby the joint campaign command headquarters, in a unified manner, task-organizationally groups a large portion of IO strengths into an IO group {*jituan*} (grouping {*qun*}), and the remainder of the IO strengths are under the control and employment of each service and arm.

(i) IO group (grouping). This is normally task-organized from IO units attached by higher-level or directly subordinate to the campaign as well as some IO strengths transferred {*choudiao*} from each service and arm. This mainly includes electronic confrontation units, network warfare units as well as local IO strengths, etc., and these are directly controlled and employed by the joint campaign command headquarters. One normally task-organizationally groups then into the IO reconnaissance grouping, radar jamming grouping, communications jamming grouping, network attack grouping, early warning aircraft confrontation grouping, satellite confrontation grouping, electronic air defense grouping and the IO reserve force, etc. They mainly undertake the missions of seizing joint campaign (localized) information dominance and supporting {*zhiyuan*} and complementing the campaign activities of other services and arms. They are normally separately deployed in areas-zones facilitative for carrying out operational missions.
[End of page 147]

(ii) On-land operations group IO grouping. This is normally task-organized from the IO strengths within the military-area-command's established structure and/or augmented by higher levels, and it is task-organizationally grouped into a number of sub-groupings based on specialty or mission. They mainly undertake on-land IO operational missions and are separately deployed in [land] zones {*diyu*} facilitative for carrying out missions.

(iii) At-sea operations group IO grouping. This is normally task-organized from the IO strengths within the Navy's established structure, and it is task-organizationally grouped into a number of sub-groupings based on specialty or mission. They mainly undertake at-sea and in-shore IO missions, and they are separately deployed in [land] zones {*diyu*} facilitative for carrying out missions.

(iv) Air operations group IO grouping. This is normally task-organized from the IO strengths within the Air Force's established structure, and it is task-organizationally grouped as a number of sub-groupings based on specialty or mission. They mainly undertake air and ground air defense IO missions, and they are separately deployed in [land] zones {*diyu*} facilitative for carrying out missions.

(v) Missile operations group IO grouping. It is normally task-organized from the IO strengths within the Second Artillery's established structure, and it is task-organizationally grouped into a number of sub-groupings based on specialty and mission. They mainly undertake IO support {*zhiyuan*} screening missions of the Second Artillery

base, and they are separately deployed in [land] zones {*diyu*} facilitative for carrying out missions.

The second is, based on the operational mission and with the joint campaign command headquarters controlling a smaller portion of elite IO strengths, one concentrates the task-organizational grouping into an IO task-group {*jiqun*} and the remaining larger portion of IO strengths are attached to the operations group of each service or arm and is under the control of the operations group of each service or arm.

5. Determining the time for completing IO preparations and the initiation time

The time limit for completing IO preparations must not only be earlier than the time limit for the other units to complete their preparations, but one must also ensure that the IO units will have a corresponding time to complete their operational preparations. The information attack initiation time refers to the time to concentrate and implement information attack. In the initial phase of the campaign, the time for concentrating and implementing information attack normally uses the **[end of page 148]** integrated firepower attack time {*zonghe huoli tuji shijian*} as a datum point, and depending on the situation, it can be conducted before or at the same time as the integrated firepower attack.

6. Determining the organizing of IO command

In determining the organizing of IO command, the key points are to clarify the IO departments and the directly-subordinate IO unit command post's deployment location, the time and place of set-up, and the organizing mode for communications and establishing contact during command.

Section 3: Issuing IO Missions..149

The joint campaign command organ should, in accordance with the commander's resolution and instructions in the aspect of IO, quickly formulate the IO plan and issue the IO missions to the units via the form of operational orders. One must be clear, specific and maintain secrecy when issuing IO missions.

The main content of IO orders includes: the enemy situation assessment conclusion; higher level IO intent; one's own level IO missions and the senior officer's basic resolution {*jiben juexin*}; task organization, deployment and missions of the IO group (grouping) and each service and arm operations group's {*zuozhan jituan*} (task group's {*jiqun*}) IO grouping; the time limit for completing operational preparations and the time for IO initiation; the time and place of IO command post set-up, etc.

When time is urgent or when concealing the operational intention, one can also issue missions with the form of individual orders. When issuing operational missions via

the form of individual orders, one ordinarily only transmits to the relevant unit and the content is limited to just the relevant items for that unit. **[End of page 149]**

Section 4: Formulating the IO Plan…150

The IO plan is the series of in-advance arrangements conducted by the joint campaign commander and his command organ in order to guide each service and arm in implementing joint campaign IO activities. The joint campaign commander should instruct the IO command institution to promptly, quickly and thoroughly accomplish the IO plan formulation work in accordance with the joint campaign commander's intent, the joint campaign activity general plan {*lianhe zhanyi xingdon zongti jihua*}, the IO missions and objectives to be reached, and the task-organizational grouping of IO strengths and mission differentiation. During a joint campaign, the chief of staff is normally in charge of the IO plan, and with the IO departments in the lead and the personnel of relevant departments participating in plan formulation, the chief of staff is responsible for examining and approving it.

I. The main content of the IO plan…150

The joint campaign IO plan normally includes the joint campaign IO activities plan and the joint campaign IO support plan.

(1) The joint campaign IO activities plan

The joint campaign IO activities plan is divided into the general plan {*zongti jihua*}, the sub-plans {*fenzhi jihua*} and the coordination plan {*xietong jihua*}.

1. The joint campaign IO general plan

The main content of the joint campaign IO general plan normally includes: situation assessment conclusion; higher level IO intention and one's own level IO missions; IO strength task-organization, deployment and mission differentiation; the partitioning of each operational phase, anticipated situations and activity courses of action; and command and coordination items, etc. **[End of page 150]**

(i) Situation assessment conclusion

This mainly clarifies: the deployment of the enemy's information systems, key-point target locations and main technical parameters; defensive and protection capabilities; the enemy's information attack capability; force strength task-organization; operational intention; operational goal; IO means and operational methods; potential operational activities one may adopt in each phase and each time occasion of combat.

(ii) Higher level intention and one's own level IO missions

Higher level intention mainly clarifies: the general guidance concept {*zongde zhidao fangzhen*}, principles and operational goal to be reached in the joint campaign; and higher level IO main objectives, main IO activities and methods, key-point defense and protection targets, means and methods. The missions of one's own level IO mainly clarifies the following: one's own level's IO strength task-organization, main operational targets, operational areas-zones and key-point targets and parts of defense and protection, etc.

(iii) IO strength task-organization, deployment and mission differentiation

This mainly clarifies: the task-organization and deployment of all subordinate services and arms IO strengths and attached or supporting IO strengths; the missions of each service and arm IO strengths; the main direction and targets of IO, key-points of strikes, main operational means and modes/methods, etc.; and key-points of information defense and main means, methods and measures, etc.

(iv) Partitioning of each operational phase, anticipated situations and operational activities courses of action

The partitioning of the joint campaign IO phase is ordinarily identical to the partitioning of the joint campaign phase, so under the premise of not conflicting with partitioning of the joint campaign phase, one can further partition into several small operational phases based on the needs-requirements of joint campaign IO. In formulating the anticipated situations and operational activity courses of action, one conceptualizes in-advance the battlefield situation in each phase of IO and the main operational activities of both sides as well as clarifies the main activity courses of action of the IO units. Furthermore, because IO is generally the first to start and last to conclude, outside of partitioning the IO phases in line with the campaign phase partitioning, **[end of page 151]** one should also plan the IO activities prior to initiation of the joint campaign and after its conclusion so as to safeguard {*baozhang*} the smooth initiation and conclusion of operations.

(v) Command and coordination items

This mainly clarifies: the deployment location of the IO departments and campaign's directly subordinate IO unit command posts; their set-up time; organizing of command communications; and modes of command and main coordination items.

2. The joint campaign IO sub-plans

The joint campaign IO sub-plans are the specification the IO activities plan in a given aspect of IO activities. This mainly includes: IO reconnaissance plan, information attack plan, information deception plan and the information defense plan, etc.

The IO reconnaissance plan and its contents include: the goal and missions of IO reconnaissance; key-point targets of IO reconnaissance; reconnaissance means and methods to be adopted; task-organization, deployment and task differentiation of the IO reconnaissance force-strengths; support measures, etc.

The information attack plan and its contents include: the key-point targets, sequence and methods of information attack; task-organization, deployment and mission differentiation of the information attack strengths; provisionally delegated information attack missions to other operational strengths; non-specialized IO strengths missions and their organizing methods; employment authority and time-opportunities for IO reserve forces.

The information deception plan and its contents include: the goal and missions of information defense; task-organization, deployment and mission differentiation of the information deception strengths; adopted deception means and methods; organization and requirements of information deception; support measures, etc.

The information defense plan and its contents include: organization and requirements of information defense; key-point targets and means of information defense; specific courses of action of information defense; coordination content of information defense; employment authority and time-opportunities of information reserve forces, etc.

On the basis of the IO form, one can also formulate an electronic warfare plan and a network warfare **[end of page 152]** plan.

3. The joint campaign IO coordination plan

The joint campaign IO coordination plan refers to the plan formulated to allow consistent adjusting-coordination action between various IO means, strengths and activities and to reduce unfavorable effects and interference between them. It is a component of the joint campaign coordination plan. [In it,] one mainly should clarify the coordination between joint campaign activities, coordination between friendly IO units, and coordination between various IO means, operational strengths, operational activities of the units at one's own level, etc. One should clarify with key-points the objectives and tasks of coordination, [clarify the] relationships between activity times with space and coordination, and [clarify] coordination measures and coordination stipulations, etc. The joint campaign IO coordination plan can be singularly formulated or it can be formulated and merged with the joint campaign IO general plan {*zongti jihua*}.

(2) The joint campaign IO support plan

The joint campaign IO support plan's main contents include: support mission differentiation; anticipated support situations; support strength disposition and activity methods; support equipment allocation and employment; command and coordination methods; time limit for carrying out tasks, etc. In the support plan, one should clarify

contents such as target support, communication support, support of classified {*jiyao baozhang*}, engineering support, electromagnetic frequency spectrum management, nuclear, biological and chemical support, position [emplacement] alert and defense, survey and mapping support, meteorological and hydrological support, battlefield management, etc.

The joint campaign IO support plan is agree upon and drafted by the joint campaign IO departments in conjunction with other relevant departments. Normally, the IO plan and the joint campaign plan are merged and formulated together, but they can also be singularly formulated. The detailed activity plan of specially designated IO is formulated by the specific implementing organizational-unit and is reported above for approval.

II. Methods for formulating the IO plan…153

Normally, one adopts the partitioning based on operational phase and a step-by-step method when formulating the IO plan. **[End of page 153]**

First step, partition the IO phases and clarify the IO tasks of each phase

When formulating the IO plan, one normally partitions the operational phases with the joint campaign phases as the basis. Afterwards, in accordance with the senior officer's resolution and campaign general activities {*zhanyi zongti xingdong*}, clarify the basic tasks of IO in each phase of the campaign.

Second step, anticipate the various IO situations and plan the various IO activities

Normally, one should, with the campaign activity general plan {*zhanyi xingdong zongti jihua*} as the basis for anticipating the campaign situation, first anticipate the various situations that may occur in the IO of each campaign phase, and then clarify the specific tasks of each IO unit in different situations and the operational activities and various coordination items one should adopt.

Third step, form the operational planning document {*zuozhan jihua wenshu*} and promptly conduct revisions, improvements and report to higher authorities

Promptly form the relevant contents into the operational planning document, and promptly report this to the chief of staff for examination and approval. When the chief of staff puts forth revision suggestions, one should promptly conduct revisions and improvements, and finally report this to the joint campaign commander for approval.

For the IO plan forms {*xingshi*}, one mainly has the written record form {*wenzi jishu shi*}, tabular form {*biaoge shi*}, annotated map form {*ditu zhuji shi*}, overall planning chart {*tongchoutu shi*}, multi-media form {*duo meiti shi*}, etc. One can also

combine several forms, for example, the written record form with the tabular and annotated map forms.

III. Requirements for formulating the IO plan…154

In formulating the IO plan, one should, with the senior officer's campaign resolution as the basis, earnestly comprehend the higher level intent, completely analyze the battlefield situation, scientifically predict battle situation developments, and formulate an IO plan that conforms to battlefield realities.

The joint campaign IO department should, after receiving {*jieshou*} the in-advance order and receiving-accepting {*shouling*} the operational missions, formulate the IO plan. Normally, one first drafts the initial plan so as to safeguard {*baozhang*} that the units smoothly conduct operational preparations. After the senior officer sets the campaign resolution, then, in accordance with the needs of joint campaign operations, **[end of page 154]**, gradually revise, replenish and improve so as to allow adjusting-coordination between the IO plan and the joint campaign operations plan; establish a foothold in the most complex and difficult situations, be adept in forecasting the possible developments and changes to the battlefield situation and conceptualize a variety of courses of action; perform unified planning {*tongyi jihua*}, perform unified operations research-based planning {*tongchou anpai*} and arrangements, and successfully plan with key-points the IO activities and critical time-occasion activities that have a significant effect on the overall situation of operations; be thorough and detailed, allow for the unforeseen, and have flexibility and adaptability; one must conduct campaign calculations, successfully calculate for essential factors such as targets, strengths, times, activities, support, etc., and one must quantify, level-by-level, the operational units and specific operational activities; when conditions exist, one should utilize computers to conduct simulation verifications; when the situation is urgent of time is short, one can draft, issue and conduct activities at the same time. After the plan is formulated, one must strictly pay attention to maintaining secrecy.

Section 5: Organizing IO Coordination…155

Joint campaign IO coordination refers to the consistent adjusting-coordination of activities adopted by IO units to accomplish their operational missions; its goal is to allow the various IO strengths to bring into play an integrated-whole might and to strive for operational victory. The joint campaign commander and his command organ should, on the basis of the joint campaign operations resolution {*lianhe zhanyi zuozhan juexin*}, the joint campaign activity general plan {*lianhe zhanyi xingdong zongti jihua*} and the joint campaign IO general plan {*lianhe zhanyi xinxi zuozhan zongti jihua*}, thoroughly organize joint campaign IO coordination.

I. Organizing the coordination sequence…155

Organizing the sequence of IO coordination includes: convening the coordination meeting, issuing the coordination instructions, and organizing coordination exercises.

(1) Convening the coordination meeting

The time-opportunity for convening the coordination meeting is normally after formulating the IO general plan **[end of page 155]** and coordination plan, and after the IO commander has already set the initial resolution {*chubu juexin*}. Ordinarily, one conducts this in a centralized manner at the main command post or at different locations synchronously by utilizing the command information system, maps or sand tables.

(2) Issuing the coordination instructions

The joint campaign IO command organ should, on the basis of the instructions of the joint campaign commander at the coordination meeting and one's own level's coordination plan, quickly draft and issue the coordination instructions. The main contents include: the content and key points of IO coordination; the missions, activities (sequence, times) of IO units in each coordination phase as well as coordination relationships; the time-opportunity and methods for establishing and dispatching the coordination institution; the means and measures of supporting coordination; measures when coordination is imbalanced or encounters disruption; coordination discipline and requirements, etc.

(3) Organizing coordination exercises

The joint campaign commander and his command organ should organize the coordination exercises in accordance with the coordination plan in order to become familiar, inspect-test, and perfect the coordination plan and support measures of coordination and allow IO units to ascertain their missions, sequences and methods in each coordination phase. Organizing coordination exercises can rely on an integrated data-link and command network for implementation.

II. Methods of organizing coordination…156

In organizing joint campaign IO coordination, one normally conducts it based on the following methods and steps: partition the coordination phases, clarify coordination tasks and coordination relationships, divide the operational areas/zones and times, and divide the electromagnetic frequency spectrum, etc.

(1) Partitioning the coordination phases

Partitioning the coordination phases refers to the partitioning of phases performed for the coordinating the operational progress. The coordination phases are normally identical to the IO activity phases. Sometimes, in order for coordination to be more clear and specific, one can further perform a more detailed partitioning into a number of time-occasions {*shijie*} on the basis of partitioning the coordination phases. **[End of page 156]**

(2) Clarifying the coordination tasks

On the basis of partitioning the coordination phases, and in accordance with the joint campaign IO goal and operational goals of each phase, perform unified clarification for the tasks of each IO unit in each coordination phase. Normally, one conducts this based on the method of first in the main direction, next in the secondary direction, first in the main activities, and next in the secondary activities.

(3) Clarifying the coordination relationships

Clarifying coordination relationships refers to clarifying the supporting {*zhiyuan*} and complementing {*peihe*} relationships between each IO unit in each coordination phase. After the coordination tasks are clarified, with the unit executing the main IO missions of each coordination phase in the lead, clarify the main-secondary relationships of coordination of each IO unit. After the coordination relationships are clear, the joint campaign commander can give authority to the operational unit shouldering the main IO missions of the various coordination phases to put forth the IO activity courses of action of their own phase as well as be responsible for performing operations research-based planning and organizing of the IO coordination of their own phase.

(4) Dividing the operational areas/zones and times

Dividing the operational areas/zones and times is the stipulations made for each IO unit in the scope of space and time for the various activities of a coordination phase. In dividing the operational areas/zones, one normally uses this when organizing each operations group (grouping) and unit are implementing operational activities at the same time. One should, on the basis of operational requirements and characteristics of the operational units, rationally partition the operational areas/zones and avoid affecting each other. In divide the operational times, one normally uses this when organizing each IO unit to carry out missions in the same space or strike the same target. One should, on the basis of the characteristics of each IO unit and the requirements on attacking targets, rationally divide the times.

(5) Dividing the electromagnetic frequency spectrum

Dividing the electromagnetic frequency spectrum refers to dividing up the electromagnetic frequency bands, and it is normally used when organizing coordination

such as early warning detection, technical reconnaissance, radio communications and establishing contact, electronic confrontation, etc. **[End of page 157]** One should, on the basis of such things as the operational missions, battlefield electromagnetic environment and information system performance, correctly divide the electromagnetic frequency bands as well as their employment time-opportunities and methods, and clarify coordination relationships and requirements.

III. Content of organizing coordination…158

In organizing joint campaign IO coordination, the key points are the coordination between the joint campaign IO group (grouping) and other operations groups (groupings), between the joint campaign IO groups (groupings) internally, and between the joint campaign IO group (grouping) and other operations group (grouping) IO units. In joint campaign IO coordination, the main body, key points and modes are different within different campaign IO activities.

(1) IO reconnaissance coordination

1. Electronic confrontation reconnaissance coordination

In electronic confrontation reconnaissance coordination, with the activities of the IO group's (grouping's) electronic confrontation reconnaissance strength activities in the lead and participation from each associated operations group, one normally organizes it based on the method of dividing by targets or one can also organize it based on the method of dividing the electromagnetic frequency spectrum and time. When organizing coordination based on the division by target method, the IO group (grouping) implements electronic confrontation reconnaissance mainly against the enemy's important targets such as command and control systems, early warning detection systems, and communication systems. The IO reconnaissance strengths of each associated operations group (grouping), on the basis of the target distribution situation and operational tasks, implements reconnaissance against the IO targets of the enemy it currently faces. When necessary, through the use of some force-strengths and firepower, each operations group (grouping) guards against the enemy conducting firepower strikes and electronic jamming on our IO reconnaissance strengths. When organizing coordination based on the division of the electromagnetic frequency spectrum method, one mainly divides the frequency bands of electronic confrontation reconnaissance and employment of electronic jamming so as to avoid affecting the results of electronic jamming reconnaissance. When organizing coordination based on the time method, one mainly divides the time-opportunities of each operations group's electronic reconnaissance and jamming activities; when implementing electronic confrontation reconnaissance, one should stop electronic jamming activities against the targets being reconnoitered, and thus ensure one's reconnaissance results.

2. Computer network reconnaissance coordination

In computer network reconnaissance coordination, with the activities of the IO group's (grouping's) computer network reconnaissance strengths in the lead and with participation from special network warfare strengths {*tezhong wangluozhan liliang*}, one normally organizes it based on the method of division of tasks. The IO group (grouping) mainly through modes such as hacker sneak-ins, special software, electronic eavesdropping and utilizing seized enemy equipment, one steals the various information from the enemy's campaign information systems and computer networks; special network warfare strengths are mainly responsible for sneaking into the enemy' rear area vital site departments {*houfang yaohai bumen*} (such as command posts, information centers, etc.) or land zones {*diyu*}; inserting virus programs into the enemy's computer systems or directly conducting electromagnetic eavesdropping reconnaissance; when necessary, each associated operations group safeguards {*baozhang*} the reconnaissance activities of the IO group (grouping) and special operations group (grouping) with some force-strengths and firepower.

(2) Information attack coordination

1. Electronic attack coordination

In coordination of electronic attack activities, with the activities of the IO group's (grouping's) electronic attack strength in the lead and participation from each associated operations group (grouping), one normally organizes according to the division by target method, but one can also organize it based on division by electromagnetic frequency spectrum, time and area-zone. When organizing coordination based on the division by target method, the IO group (grouping) mainly implements electronic attack against the enemy, disrupts and weakens the operational effectiveness of important information systems such as the enemy's communication systems, early warning detection systems and command and control systems, and seizes electromagnetic superiority. The electronic attack strengths of each associated operations group (grouping) implements electronic jamming and suppression against the each type of information system of the enemy they are facing on the basis of operational missions of their own group (grouping). Amongst this, special operations task group {*tezhong zuozhan jiqun*} sneaking into the enemy's rear area implements disruption-raid activities against the important targets that cannot be effectively suppressed by electronic attack. When necessary, each associated operations group (grouping) guards with a portion of their operational force-strengths and firepower against the enemy's implementation of firepower strikes against our electronic attack strengths. When we implement electronic attack activities, **[end of page 159]** the IO reconnaissance strengths of each operations group (grouping) should continue to conduct reconnaissance against the enemy's important targets, and to understand and grasp the results of our attack activities. When organizing coordination based on division of electromagnetic frequency spectrum method, one mainly divides up the frequency spectrum used to implement electronic jamming against the enemy from the frequency spectrum of our equipment employed by units having electronic equipment, so as to

avoid unfavorable effects upon our operational activities. When organizing coordination based on the division of time method, one mainly ascertains the priority sequence for implementing electronic attack against the enemy's important electronic targets by each operations group (grouping). When organizing coordination by division of areas-zones, one mainly clarifies the areas-zones and directions for implementing electronic attack activities against the enemy by each operations group (grouping).

2. Computer network attack coordination

In computer network attack coordination, with the activities of the IO group's (grouping's) computer network attack strengths in the lead and with participation of special operations group (grouping) and other associated IO groups (groupings), one normally organizes this based on the division by mission method. The IO group (grouping) mainly implements attacks against the enemy's computer networks and systems via modes such as hackers and infiltrations, etc.; they decrease and destroy the functions of the enemy's information processing systems; and paralyze and weaken the operational effectiveness of the enemy's command and control capabilities and information weapons and equipment. The special operations group (grouping) is mainly responsible for sneaking into the enemy's rear, approaching or directly entering the enemy's computer network systems, and implementing disruption and destruction. When necessary, each associated operations group (grouping) safeguards {*baozhang*} the activities of the IO group (grouping) and special operations group (grouping) with a portion of their operational force-strengths.

3. Coordination of conducting firepower strikes against the enemy's information systems

In the coordination of conducting firepower strikes against the enemy's information systems, with the activities of the IO group's (grouping's) information attack strengths in the lead and participation by the on-land, at-sea, air and Second Artillery operations groups {*zuozhan jituan*} and special operations task group {*zuozhan jiqun*}, one normally organizes based on the division of targets method. One ordinarily implements firepower strike activities against the enemy after electronic attack, but one may conduct it simultaneously mainly to directly conduct firepower strikes against targets with bad results **[end of page 160]** from electronic attack; this further disrupts and thoroughly destroys the important targets such as the enemy's command and control centers, electronic information systems, and early warning radar systems, etc. The Second Artillery operations group mainly destroys the enemy's in-depth command systems and important electronic targets, communication hubs, etc.; the on-land operations group mainly destroys the enemy's command posts, radar stations, radio jamming platforms and communication network platforms deployed near the forward edge; the air operations group mainly destroys the important electronic targets and early warning aircraft in the enemy's depths; the special operations task group mainly implements harassment and disruption against targets such as the enemy's communication hubs, radar stations, command centers, etc. When conducting strikes

against the enemy, the information attack strengths of the IO group (grouping) should conduct jamming and suppression against the enemy's anti-missile systems, early warning radar systems, fire control radar systems, etc. and safeguard the smooth penetration and sustained strikes of our firepower strike strengths; the IO reconnaissance strengths should continuously conduct reconnaissance against the enemy's important targets and comprehend and grasp the effects of our firepower strike activities so as to provide a reliance for further implementing strikes.

(3) Information defense coordination

1. Coordination for defending against the enemy's information reconnaissance

Defending against enemy reconnaissance coordination. With the main operations group's (grouping's) information system protection strength in the lead and with participation from other relevant operations groups (groupings), one normally organizes this based on the method of division of tasks. The main operations group (grouping) information system protection strength is responsible for ensuring our important information system's safety {*anquan*} and information security {*baomi*}. When the enemy implements information reconnaissance, each associated operations group's (grouping's) information attack strength should temporarily maintain radio silence so as to avoid revealing early our actual strength and activity intention, and under certain conditions, they can also implement jamming and disruption against the enemy's information reconnaissance systems; the information reconnaissance strengths should unfold anti-reconnaissance activities at the appropriate time, and find out the deployment and parameters of the enemy's electronic reconnaissance weaponry as well as the enemy's operational intent, etc. Each associated operations group (grouping) should, depending on the situation, implement firepower strikes against the enemy's information reconnaissance weaponry and disrupt their reconnaissance activities; or [they should] implement force-strength feints **[end of page 161]** and deceive and confuse the enemy.

2. Coordination for defending against the enemy's electronic attack

Defending against the enemy's electronic attack coordination is performed with the main operations group's (grouping's) information system protection strength in the lead and with participation from other associated operations groups (groupings); one normally organizes this based on the method of division of tasks. The main operations group's (grouping's) information system protection strength is responsible for ensuring our important information systems' safe and stable operations and normal bringing into play of their functions each associated operations group's (grouping's) electronic jamming strength is responsible for implementing jamming and suppression against the enemy's information attack weaponry. Within this, the IO group's (grouping's) electronic jamming strength should implement counter-electronic jamming in the main direction and in the zones where important protection targets are deployed; the information reconnaissance strength unfolds reconnaissance activities at the right time against the enemy, finds out the deployment and parameters of the enemy's electronic attack

weaponry so as to facilitate our adoption of effective measures for conducting counterattack activities; each associated operations group's (grouping's) firepower strike strength should, depending on the situation, conduct firepower strikes against the enemy's electronic attack weaponry and disrupt their electronic attack activities.

3. Coordination for defending against the enemy's computer network attacks

In coordination for defending against the enemy's computer network attacks, with the activities of the IO group's (grouping's) computer network defense strength in the lead and with participation from each associated operations group (grouping), one normally organizes this based on the method of division of tasks; the IO group's (grouping's) computer network defense strength is mainly responsible for organizing activities such as defending against the enemy's hacker attacks, virus attacks and preventing electromagnetic leaks, etc., for preventing the enemy from utilizing their computer networks to disrupt our information systems, and thus ensuring our network's safety; the computer network attack strength is responsible for implementing attacks against the enemy's networks and achieve the goal of assisting defense through offense; other associated operations groups (groupings) are responsible for the reinforcing the protection within our computer network zones with a portion of force-strengths; and mainly to strictly defend against the enemy's special units from penetrating through and implementing disruption activities against our computer networks.

4. Coordination for defending against the enemy conducting firepower strikes against our information systems

In coordination for defending against the enemy conducting firepower strikes against our information systems, with the activities of the main operations group (grouping) **[end of page 162]** in the lead and participation from each associated operations group (grouping), one normally organizes this based on the method of division of tasks. The main operations group (grouping) is responsible for synthetically applying various means to organize protection and resistances and for ensuring the safety of our information systems; each associated operations group's (grouping's) firepower strike strength is responsible for conducting resistance-attacks and counterattacks against the enemy's firepower strike weaponry and platforms, and for wiping out the special operations units (elements) penetrating our depths; the IO group's (grouping's) electronic jamming strength is responsible for implementing jamming against the enemy's precision guidance weapon systems, influence their hit results, and screen the safety of our important military targets and important electronic information systems.

IV. Requirements of organizing coordination…163

At the same time as the joint campaign commander and his command organ organize IO coordination, one normally should grasp in general terms the following issues:

(1) Focus on the overall situation, and conduct integrated-whole adjusting coordination

One must focus on the overall situation of the joint campaign, center on the general campaign tasks, combine the basic fighting methods and the real situation of the given campaign, and conduct integrated-whole adjusting coordination for the IO activities throughout the entire course of the campaign of each operations group (grouping), each type of campaign pattern, each battlefield and in each campaign direction. Further make specific the IO tasks, and determine the IO targets and tasks one must achieve from the overall perspective as well as the priority sequence for reaching the IO objectives. [One must] conduct unified operations research-based planning and arrangements in terms of the sequence and methods for campaign tasks, strengths employment, operational areas-zones, times and campaign activities for each campaign pattern, each battlefield and campaign IO activities of each campaign direction, thus being able to allow for consistent adjusting-coordination from the integrated-whole perspective and the campaign activities of each campaign large formation, in particular the activities of the main direction's campaign large formation.

(2) Grasp the layers, and give prominence to coordination key points

One must clarify with key points the coordination content, coordination relationships and coordination requirements between IO activities and other campaign activities, and [one must] successfully grasp the coordination layers between the IO activities of the operations group (grouping) **[end of page 163]** of each service and arm, each campaign direction and various campaign patterns. Their internal campaign IO coordination is normally organized by the subordinate levels.

For organizing joint campaign IO coordination, in terms of IO strength employment, one must use the strengths carrying out the main missions as the key point; in terms of organizing the implementation of IO activities, one must use the main campaign patterns as the key point; in terms of the adjusting-coordination of operational spaces, one must use the IO activities of the main battlefield and main campaign direction as the key points.

(3) With planned coordination in the lead, flexibly organize ad hoc coordination

The modes of joint campaign IO coordination are normally with planned coordination {*jihua xietong*} in the lead and a combination of planned coordination and ad hoc coordination {*suiji xietong*}.

Planned coordination is complete and thorough, and it has an overall-situation quality guidance role for the coordination of each phase of the campaign. When formulating the joint campaign IO coordination plan, one must place the point of focus on the overall situation issue and the key point issues; and for the specific campaign course coordination issues, one should make macroscopic and principal-quality

stipulations so as to leave sufficient room for ad hoc coordination during the campaign course. Ad hoc coordination is normally conducted by aiming at the local situations of the campaign course, and it has a stronger adaptability for changes of the battlefield situation. When the situation exceeds the scope of the coordination plan or if the original plan does not suit the given actual situations, one should flexibly organize ad hoc coordination. For organizing ad hoc coordination, one can make adjustments or alter the original coordination plan based on the new situation; when there are no fundamental changes occurring in the development progress of the campaign, the ad hoc coordination must still be conducted and organized in accordance with the original coordination tasks and original principles.

(4) Adopt a variety of measures, and maintain uninterrupted coordination

In joint campaign IO coordination, its contents are many while its relationships are complex, and it can be easily disrupted during the course of the campaign. For this reason, one should adopt the following measures: first is perfecting the coordination mechanism {*wanshan xietong*}. The joint campaign command headquarters organizes the planning of the employment of the participating IO strengths in a unified manner. It conducts a unified planning for the operational activities of the IO units of each service and arm as well as performs unified coordination for the IO and other operational activities. One can consider setting up an IO adjusting-coordination team within the joint campaign command headquarters IO department to be composed from personnel dispatched from participating IO departments of each service and arm; it [IO adjusting-coordination team] is represented by associated departments such as intelligence and communications, and it organizes the campaign IO coordination in a unified manner. Second is strengthening consultations [with each other] {*jiaqiang xieshang*}. The IO units of each service and arm having IO coordination relationships should, on the basis of the IO coordination plan and instructions, promptly conduct consultations [with each other] and resolve with key points any specific coordination issues. Consultations can be organized by the joint campaign command institution dispatching of personnel or by designating the commander of a certain campaign large formation to be responsible for organizing it. After consultations, one should form the activity course of action {*xingdong fang'an*} each side must abide by in coordination; each side participating in the coordination should, on their own initiative, organize activities based on the agreed upon items and ensure their implementation. Third is strengthening analysis and forecasting and improving one's ability to adapt. Taking aim at the specific changing situations of the joint campaign IO battlefield situation, promptly adjust the original coordination contents and allow the participating IO units of each service (or arm) to maintain uninterrupted coordination from start to finish.

Section 6: Organizing Synthesized Support {*zuzhi zonghe baozhang*}…165

After formulating the IO plan, the joint campaign commander should, at the appropriate time, guide the IO departments to organize operational, logistic and equipment support and to clarify with key points support tasks, support relationships, key

points and requirements. In organizing various supports, one should adhere to the principles of have preparations in advance; perform unified operations research-based planning and deal with all things; complete support; and give prominence to key points. [In organizing various supports, one should] actively create and fully utilize various favorable conditions; synthesize the application of various support modes and methods; bring into play the integrated-whole composite might of all services and arms and local support strengths.

I. Organizing operational support…165

The joint campaign commander and his command organ should put operations support of the joint campaign into the joint operations plan, and organize its implementation in a unified manner. Normally, **[end of page 165]** the joint campaign IO command institution puts forth the IO support requirements and the relevant support departments organize the implementation according to plan. After the IO support plan is formulated, one should promptly issue the corresponding operational support instructions. On the basis of the instructions of higher level and their own level's commanders, the IO support plan as well as the IO needs-requirements, organize in a unified manner the operational supports such as target support, communications support, classified security support, engineering support, electromagnetic frequency spectrum management, nuclear-biological-chemical support, position alert and guarding and survey-mapping support, meteorological-hydrological support, battlefield management, etc.; perform guidance, control and adjusting-coordination for the various IO support strengths, flexibly apply modes such as a combination of specialized support strengths with non-specialized support strengths and a combination of standard production {制式 *zhishi*} and non-standard {*fei zhishi*} equipment and instruments, and completely unfold support activities with key points.

II. Organizing logistic support…166

The joint campaign commander and his command organ should put the logistic support of joint campaign IO into the joint campaign logistic support plan and organize its implementation in a unified manner. Normally, the joint campaign IO command institution puts forth the relevant IO logistic support requirements, and the associated support departments organize and implement it based on the plan. After the IO logistic support plan is formulated, one should promptly issue the IO logistic support instructions. On the basis of the higher level and one's own level commander's instructions, the IO logistic support plan and the needs-requirements of IO activities, organize in a unified manner the logistic support such as IO materiel, medical, traffic and transport and cost; perform control and adjusting-coordination for the various support activities; flexibly apply modes such as a combined area-zone support with established structure support, and a combined general-use support with special-use support; and unfold logistic support activities.

IV. Organizing equipment support…166

The joint campaign commander and his command organ should put the equipment support of joint campaign IO into the joint campaign equipment support plan, and organize and implement it in a unified manner. Normally, the joint campaign IO command institution puts forth the relevant IO equipment support requirements, **[end of page 166]** and the associated support departments organize and implement in accordance with the plan. After the IO equipment support plan is formulated, one should promptly issue the IO equipment support instructions. On the basis of the higher level and one's own level commander's instructions, the IO equipment support plan and the IO activity needs-requirements, organize in a unified manner the IO equipment materiel, technical, management and cost supports. Perform control and adjusting-coordination for the various IO equipment support activities; flexibly apply modes such as area-zone support with established structure support, unified support with separate support, planned support with emergency support, level-by-level support with skip-echelon support, etc.; and unfold equipment support activities.

Section 7: Organizing Wartime Political Work…167

In organizing wartime political support, one should put IO political work into the joint campaign political work plan and organize and implement it in a unified manner. After the wartime IO political work plan is formulated, one should promptly issue the IO political work instructions. The joint campaign commander and his political organ should, on the basis of the IO missions, guide each operations group's (grouping's) IO units to take aim at the IO characteristics and promptly and thoroughly conduct political mobilization and propaganda education; use the orders and instructions of the Party Central Committee, the CMC and higher levels to unify the thought and activities of combat-participating personnel; allow the collective combat-participating personnel to comprehend higher level intent; clarify the IO goals, missions, meaning, favorable factors and unfavorable conditions as well as the methods for gaining victory and subduing the enemy; thoroughly conduct patriotism, collectivism and revolutionary heroism education; and arouse combat-participating enthusiasm and combat spirit. Organize and unfold the organizing work and cadre work as well as the activities of military democracy and establishing a model of meritorious service; organize the implementation of psychological warfare, public opinion warfare and legal warfare; and successfully accomplish the mass work in the operations area. **[End of page 167]**

Section 8: Organizing IO Unit Unfolding…168

IO unit unfolding is the activity whereby one, on the basis of the task-organization of the joint campaign IO strength, maneuvers the participating IO strengths of all services and arms to the assembly (standby) zones. The goal is to gather the operational strengths, form a favorable pre-battle posture, and ensure prompt initiation of IO. The IO strengths of each combat-participating service or arm, except for the first line electronic reconnaissance units, are ordinarily dispositioned in the shallow depths. Therefore, in the

campaign preparations phase, one should, on the basis of the campaign intent, campaign strength task-organization, pre-determined operations plan, and missions undertaken by each IO unit, under the unified command and adjusting-coordination of the joint campaign command institution, and in accordance with the operational disposition and the stipulated time, implement maneuver and unfolding of force-strengths and weaponry, enter the pre-designated battle standby location, and complete the campaign unfolding.

In order to safeguard the rapid and concealed maneuvers of each IO unit, the joint campaign commander and his command organ should guide the IO units, and on the basis of the general maneuver and unfolding resolution and proposal, set the IO unit maneuver and unfolding resolution. The main contents of the maneuver and unfolding resolution are: the goal and tasks of maneuver and unfolding, the maneuver routes, maneuver disposition, maneuver sequence, departure start time, arrival time limits, unfolding area, communications and maintaining contact, organizing of command and various support measures, etc.

The maneuver route {*jidong luxian*}. Normally, one should partition the maneuver route based on the terrain of the operations area, condition of the roads and deployment locations of each IO grouping {*qun*} with each IO grouping as the organizational-unit {*danwei*}. When two or more organizational-units are maneuvering on the same route, one should divide up the maneuver time.

The maneuver disposition {*jidong bushu*}. This should be determined on the basis of the pre-determined operational disposition and the maneuver road conditions; one normally separately maneuvers along different directions and multiple roads and multiple echelons. Based on the situation, each **[end of page 168]** IO reconnaissance grouping can maneuver before other IO groupings, while each IO grouping can move in at the same time as the reserve forces or after.

The maneuver mode. In organizing IO unit maneuver across areas-zones, the distances are long, time is urgent, modes many and organization and command are more complex. Normally, one should, on the basis of the campaign missions and deployment locations, combine the current enemy situation, traffic support and one's own maneuver capabilities, synthesize the application with a variety of modes such as public roads, railroads and aerial transport, prepare a variety of maneuver preliminary proposals {*jidong yu'an*}, rapidly make a selection based on the battlefield situation, and flexibly implement it; on the basis of the actual situation of the unit's peacetime dispersed disposition, simultaneously organize multiple echelons {*duoge tici*} from several directions with a variety of modes to quickly move into the operational zones; task-organize the units in the same direction of maneuver into a number of marching echelons {*xingjun tidui*} following multiple routes and divided into many echelons, they disperse and move in towards the operational areas-zones.; one can also synthesize the application of the aforementioned modes, adopt modes such as a maneuver that is a blended task-organizational grouping {*bianzu*}, a maneuver of multiple roads and multiple directions, batch-by-batch maneuver, seeking gaps segment-by-segment maneuver, etc.

When organizing maneuver and unfolding, the IO command institution must be under the unified plan of the joint campaign command headquarters, scientifically calculate and select the favorable maneuver time-opportunity, and allow each service and arm IO strength to be able to arrive at position in a concealed and rapid manner and on time; on the basis of completely analyzing the situations of both sides, and from needs-requirements and possible departure, weigh the battlefield conditions, strive to select the maneuver routes where concealment and maneuver conditions are better, thus facilitating maneuvering in multiple batches, multiple directions and multiple echelons and as much as possible avoiding areas-zones where one easily encounters enemy detection and raids; in order to allow for concealed, rapid and safe maneuver of each IO unit (element), one should adopt various measures to conduct reliable support. As much as possible utilize the dark of night, bad weather and favorable terrain, adopt technical camouflage means, and complement with electronic feints and deception, manufacture false intelligence, set up false targets, strictly blockade news information, successfully accomplish traffic and protection support and logistic support, and ensure the safe, smooth and concealed accomplishment of campaign unfolding.

After the units arrive at the assembly (standby) zones, one should conduct in-depth and echelon deployments according to the operational disposition and priority order for entering into engagements, **[end of page 169]** successfully accomplish concealment camouflage, and quickly complete operational preparations.

Section 9: Organizing Imminent Battle Training and Supervision of Operational Preparations…170

During the campaign preparations phase, the joint campaign commander and his command organ should promptly organize their subordinate IO units to conduct directed-quality imminent battle training and earnestly supervise and inspect the units as they complete operational preparations.

I. Organizing imminent battle training…170

Prior to campaign initiation, the IO group (grouping) and the IO units of each service and arm should conduct directed-quality training on the basis of their own operational missions, operational characteristics, and the theater's natural geographical and meteorological-hydrological situations.

In imminent battle training, one mainly conducts the following directed-quality training: first is new type weapons and equipment training. Based on the IO missions, operational characteristics and fighting methods of the operational object, supervise-urge and guide each IO unit to conduct strengthening of imminent battle familiarization and mastery of new-type weapons and equipment training, as quickly as possible achieve organic combination of man and weapon and form combat power. Second is IO fighting method confrontation training. Based on the IO fighting method put forth in the IO resolution and while directed at the object of operations and the IO tasks of the unit,

organize the unit to conduct the corresponding IO fighting method confrontation training so as to allow the unit to be able to proficiently grasp and apply IO fighting methods. Third is IO coordination training. Based on the missions and mutual coordination relationships of each unit in each phase of operations entrusted by the IO resolution and plan, organize and guide the units to conduct coordination training, reduce coordination mistakes and improve the IO strength's capability in coordinated operations.

For the procedures and methods of organizing imminent battle training, normally, on the basis of the IO task-organizational grouping {*bianzu*} and missions, **[end of page 170]** one first learns theory and unifies thought, and then one conducts real exercise training; first, each IO grouping {*qun*} performs separate training, then the IO group {*jituan*} (grouping {*qun*}) performs combined training {*helian*}; first conduct exercises on the map, sand table and computer, then conduct live force exercises. The various imminent battle training should pay attention to not reveal PLA operational intention.

In organizing imminent battle training, one must adhere to the characteristics of time urgency, many in content, and high in requirements, and thoroughly plan and strictly organize it; on the basis of peacetime training, one must give prominence to the urgently needed key point and difficult point subjects training and especially coordination training; one must undergo imminent battle training, and inspect-test and perfect the IO plan; IO imminent battle training should simultaneously organize and implement combined information deterrence and feint-deception simultaneously.

II. Supervising operational preparations…171

During the course of operational preparations as well as after basically completing operational preparations, the joint campaign commander and his command organ should instruct the IO command institution to organize the supervision and inspection of IO units at the appropriate times to complete their operational preparations.

The contents of supervising operational preparations normally include: the comprehension level of the IO units of each service and arm for the IO resolution and instructions; whether each IO unit's resolution and plans conform to the senior officer's intent; whether operations, logistic and equipment support and political work conform to higher level instructions and the requirements of the unit's operational missions; the comprehension level for the IO coordination plan; the organizing situation of the command post and the command information systems; and other situations in completing IO preparations, etc.

Supervising operational preparations normally adopts the following methods: the commander himself inspects the units; the commander or the command institution sends an inspection team to the units for inspection; listening to subordinate level reports on the imminent battle preparations; inquiring and checking-approving the documents and reports concerning IO preparations; utilizing battlefield real-time monitoring systems to conduct monitoring and provide feedbacks.

Supervising operational preparations should give priority to the IO units **[end of page 171]** executing the main IO missions; give prominence to the key points of supervision and for issues discovered during inspection and situations made known by the unit, one should promptly resolve them. Normally, one should resolve upon discovery, but for significant problems, one can centralize and resolve them in a unified manner. Issues unable to be resolved at one's own level must be promptly reported to higher levels and request higher levels to resolve them. For lower level IO resolutions and plans that do not correspond to reality nor conform to the general operational intent {*zongde zuozhan yitu*}, one must explicitly make corrections. **[end of chapter]**

This page intentionally left blank.

Chapter 9
Implementation of Joint Campaign Information Operations…173

Implementation of joint campaign information operations [IO] is the series of IO activities unfolded that relies on the joint campaign IO resolution and plan and mainly centers on IO reconnaissance, information attack and information defense. During its implementation, one should carry out the principles of *be guided by reconnaissance* {*zhencha xiandao*}, *combine attack and defense* {*gong-fang jiehe*}, and *give priority to attack* {*yigong weizhu*}; concentrate the employment of IO strengths in the main direction and important time occasions {*zhongyao shijie*}; strike with key points the vital site parts of the enemy's information systems; simultaneously organize successfully the protection of one's own information systems; and strive to seize and maintain localized information dominance.

Section 1: IO Reconnaissance Activities {*xingdong*}…173

In IO reconnaissance is mainly the reconnaissance activity {*zhencha huodong*} adopted that is backed up by the joint campaign intelligence reconnaissance *tixi* system in order to collect the needed intelligence for IO. It is the foundation for implementing information attack activities {*xingdong*}, and it has an important role in correctly setting the IO resolution and rationally employing IO strengths.

I. IO reconnaissance missions…173

The goals of IO reconnaissance are to provide reliable information intelligence for the commander to correctly set the IO resolution and even the joint campaign resolution, to promptly provide intelligence data to each service or arm participating in combat, and to create conditions for implementing IO. Its main missions are: **[end of page 173]** to ascertain the enemy's IO intention, plans and courses of action {*jihua fang'an*}, and activity disposition {*xingdong bushu*}; the types, deployment {*peizhi*}, performance and employment means of the enemy's reconnaissance monitoring systems, in particular the situation of the IO system's critical nodes {*guanjian jiedian*} as well as the methods and measures of their information defense; the main means and strengths of the enemy's information systems implementing attacks against us; the situations of the utilizable civilian information system facilities and equipment; simultaneously and actively gather the reactions of associated nations towards our joint campaign IO; and other information reconnaissance missions, etc.

II. IO reconnaissance activities {*xingdong*}..174

IO reconnaissance activities can ordinarily be divided into activities such as electronic confrontation reconnaissance, radar reconnaissance, radio technical reconnaissance, network reconnaissance, etc.

(1) Electronic confrontation reconnaissance

In electronic reconnaissance, one mainly applies electronic confrontation reconnaissance equipment, gathers and acquires the electromagnetic emanation signals of the enemy's electronic equipment, and through analysis and identification, one gathers their tactical and technical parameters and their data situations. The first is radar confrontation reconnaissance. For this, one mainly employs various equipment of radar confrontation reconnaissance to form a radar confrontation reconnaissance network {*leida duikang zhencha wangzhan*}, adopts a variety of position-fix methods and means, determines the enemy's radar locations, and ascertains the technical parameters and tactical characteristics of the enemy's radars. Second is communications confrontation reconnaissance. One mainly employs a variety of means such as fixed or mobile ground stations and electronic confrontation reconnaissance aircraft and methods such as radio communications monitoring, direction finding and position fixing to search for the enemy's radio communication signals and ascertain the enemy's radio communication equipment locations. Third is electro-optical confrontation reconnaissance. One mainly utilizes various equipment of electro-optical confrontation reconnaissance, adopts modes such as laser confrontation reconnaissance and infrared confrontation reconnaissance, and acquires the enemy's electro-optical emanation source signals and target infrared emanation signals. Fourth is hydro-acoustic confrontation reconnaissance. One mainly utilizes various installed equipment for sonar detection to conduct search, direction-finding and position fixes, identification and tracking of targets in the water and support the smooth implementation of at-sea IO.

(2) Radar reconnaissance

In radar reconnaissance, one mainly utilizes radars such as battlefield reconnaissance radars, ground-to-air intelligence radars, **[end of page 174]** surface-to-sea alert radars, ground artillery radars and early warning radars to conduct long range, all-weather, rapid and highly precise reconnaissance against the enemy so as to provide long range air situations. Amongst these, the battlefield reconnaissance radar mainly provides reconnaissance for Army units and it monitors the enemy's vehicles and personnel on the battlefield; the ground-to-air intelligence radars include alert radars, target indication radars and vector-guidance radars mainly to be used to search for, detect and identify air targets; the surface-to-sea alert radars are ordinarily installed on various types of sea surface ships or installed on shore or islands and are used for detecting sea surface ships and flying targets at low altitudes or very low altitudes.

(3) Radio technical reconnaissance

In radio technical reconnaissance, one mainly conducts reconnaissance activities through electronic reconnaissance satellites, electronic reconnaissance aircraft, electronic reconnaissance boats, ground reconnaissance stations and air-dropped electronic reconnaissance equipment. It mainly includes radio communication signals reconnaissance and non-communication signals reconnaissance. Radio communication

signals intelligence mainly applies means such as radio reconnaissance to receive, monitor, direction find, signals analysis, code-breaking, comprehensive check translation {综合校译 *zonghe jiaoyi*}, it ascertains with key points the enemy's IO intention, activity disposition, command and control system composition and deployment, and technical parameters of important weapons and equipment. For non-communication signals reconnaissance, one mainly applies non-communication signals reconnaissance means to conduct reconnaissance surveillance and analytical processing for the enemy's signals such telemetry, remote control, remote sensor, radar, navigational guidance and identification friend or foe, and space targets {*kongjian mubiao*} etc; it ascertains with key points the situations such as the composition, disposition and technical parameters of the enemy's systems such as the missile early warning, radar detection, and weapons control, as well as space target operating orbits, etc.

(4) Network reconnaissance

In future PLA joint campaign IO implemented against the enemy, in order to utilize computer networks to conduct "virus" attacks against the enemy, we must first grasp the situations such as their software types, structural functions, work processes, weak links and protection measures, and only by grasping these situations will we be able to develop {*yanzhi*} "viruses" with a focused quality to attack-enter the enemy's networks or conduct protection with a focused quality. Network reconnaissance is the activity of conducting reconnaissance against computer networks through specific reconnaissance **[end of page 175]** technologies {*zhencha jishu*} and entering the enemy's computer networks using legitimate user identification {*yi hefa yonghu shenfen*}; it is mainly to conduct searches {检索 *jiansuo*}, browsing {浏览 *liulan*}, cutting sections {截取 *jiequ*}, modifying {修改 *xiugai*} and deleting {删除 *shanchu*} on-line data and documents {*wangshang ziliao, wenjian*}. During the course of IO reconnaissance, the campaign commander and his IO command institution should at the right time organize the IO network reconnaissance strength to synthetically apply technical means such as network search {*wangluo sousuo*}, computer scans {*jisuanji saomiao*}, decoding {*mima poyi*}, signal processing {*xinhao fenxi*}, protocol decryption {*xieyi jiemi*}; they should ascertain with key points the situations such as the communication *tizhi* system, modulation-control modes, topology, network protocols, circuit security, security protection mechanisms and operating system features and distribution frailties of the enemy's computer network systems so as to provide intelligence for organizing and implementing network attacks and other operational activities.

III. Requirements of IO reconnaissance…176

IO reconnaissance possesses the characteristics of multi-elements of strength, complexity of situations, and great degree of difficulty in organizing and implementing. In order to fulfill the needs-requirements of the entirety of joint campaign operations, IO units (elements) should, based on the missions undertaken, mainly grasp the following issues during IO reconnaissance:

(1) Thoroughly plan, and meticulously perform operations research-based planning {*zhoumi jihua, jingxin chouhua*}

IO reconnaissance can not only be implemented independently, but it can also be organized and implemented while blended into all campaign reconnaissance activities under the unified plans of a joint campaign command organ. When conducting IO reconnaissance activities against the enemy's strategic depths, it is a unified organization by a joint campaign command headquarters and it is implemented mainly by employing ground, sea and air IO reconnaissance strengths possessing long range reconnaissance and surveillance capabilities within the campaign task-organization. In reconnaissance against the enemy's on-land shallow depth IO situations, one mainly employs Army IO strengths and implements it with support {*zhiyuan*} and complement from the IO reconnaissance strengths of other services and arms, and Armed Police and people and masses reconnaissance strengths. For reconnaissance of the enemy's at-sea IO situations, one mainly employs Navy IO reconnaissance strengths and implements it under the support {*zhiyuan*} and complement of sea reconnaissance strengths of other services and arms as well as those of the local area. For reconnaissance against the enemy's air IO situations, **[end of page 176]** one mainly employs Air Force IO reconnaissance strengths and implements it under the support {*zhiyuan*} and complement of the air reconnaissance strengths of other services and arms as well as those of the local area. Prior to carrying out missions, each IO reconnaissance unit (element) should establish the organization before hand and clarify responsibilities; on the basis of higher level intent, IO needs and our IO reconnaissance capability, one should determine the goals and missions of IO reconnaissance; the joint campaign IO department should, jointly with the intelligence center and centering on the main direction and important activities of IO, thoroughly formulate the IO reconnaissance plan based on the joint campaign IO plan. Its main contents include: the enemy's IO capability, main means and activity characteristics {*huodong tedian*}; PLA IO reconnaissance goals and missions; key point reconnaissance activities and targets, and adopted reconnaissance means, methods and steps; the missions of various IO reconnaissance strengths, their task-organizational grouping and support measures, etc. After the IO reconnaissance plan is determined, one should at the right time issue the campaign IO reconnaissance instructions to the units, and at the appropriate time, supervise and inspect the units to complete their reconnaissance missions according to plan.

(2) Perfect the *tixi* system, and synthetically apply

When organizing the implementation of IO reconnaissance, one must rely on the campaign reconnaissance *tixi* system, smash the phenomena of each service or arm and department doing things their own way, and in accordance with the needs-requirements of the integrated-whole of campaign IO and its requirements, [one must] establish an IO reconnaissance *tixi* system that is integration-compatible with the campaign reconnaissance *tixi* system and achieves information sharing, resource sharing and maximally satisfies IO needs-requirements. One should organize with key points the campaign IO reconnaissance strength and synthetically apply the various reconnaissance

means; one should conduct task-organizational grouping in a unified manner for the IO reconnaissance strengths of the campaign large formation subordinate units and form a collectively integrated multi-layered, in-depth, and omni-directional IO reconnaissance *tixi* system for information gathering, information transmission, information processing and information use; [this *tixi* system] is organically blended with higher level intelligence reconnaissance system {*xitong*}, thus ensuring that one is able to gather the relevant intelligence information from within the higher level intelligence reconnaissance system needed for campaign IO. **[End of page 177]**

(3) Reconnaissance in advance, and combine peacetime and wartime

Peacetime reconnaissance is the foundation for wartime reconnaissance; wartime reconnaissance is the continuation of peacetime reconnaissance; and only by grasping with key points the situations of the enemy's battlefield information functions and IO capabilities in peacetime can one be able to establish a firm basis for implementing IO in wartime. To this end, in peacetime, one should comprehend and grasp with key points the relevant situations of the enemy's IO exercises, and grasp the relevant situations of the enemy's strategic, campaign and tactical information systems and IO fighting methods; the command organs at each level should strengthen their study of contents such as IO reconnaissance organization and implementation and main means and methods of IO reconnaissance; one should strengthen campaign IO reconnaissance strength building and specialized talent cultivation and reserves while improving as quickly as possible the levels and capabilities of PLA to implement network reconnaissance; strengthen the comprehensive exercises of IO reconnaissance and improve the level and capability of the PLA to implement IO reconnaissance; adopt effective measures, revise reconnaissance plans at the right time, adjust IO reconnaissance strength dispositions, and ensure achieving rapid transitions from peacetime to wartime.

Section 2: Information Attack Activities…178

Joint campaign information attack is the series of operational activities that is combined with firepower strikes and special disruptions to seize and maintain campaign localized information dominance and it has the enemy's strategic and campaign systems and operational information as the main attack targets; its main means are electronic attack, network attack, special information warfare weapons attack, psychological attack and information deception; and its goal is to weaken the enemy's capability to gather, transmit, process and use information.

I. Information attack missions…178

The main missions of information attack are: to suppress and destroy the enemy's information gathering equipment such as radar stations, sound ranging stations, **[end of page 178]** and reconnaissance surveillance satellites; to suppress and destroy their communication hubs and command and control center and to strip away and weaken the enemy's information collection, distribution and processing capabilities. [Main missions

are to:] Combine anti-radiation and destruction to implement electronic jamming against the enemy's air defense systems and support {*zhiyuan*} our aviation force's penetration operations; implement attacks against the enemy's computer systems and computer networks and lower their operating effectiveness and network warfare capability; combine other military deception activities, implement jamming against the enemy's precision guidance weapons and guidance systems, and affect their hit results while screening the safety of our important targets; implement jamming against the enemy's GPS systems and lower their position fix precision; implement jamming, suppression and destruction against the enemy's anti-missile intercept guidance systems and the communications equipment of their anti-missile systems, and lower the operational effectiveness of the enemy's anti-missile systems while screening the penetration of our conventional missiles; combine other military deception means to implement information deception against the enemy, and thus concealing our campaign intention; implement psychological attack against the enemy, slacken and collapsing the enemy's operational will to fight.

II. Information attack activities…179

In joint campaign IO, one should, under the situation of ensuring the security and stability of our information systems, mainly adopt information attack means in order to seize local information dominance.

(1) Electronic attack

The joint campaign command and his command organ should center on weakening the enemy's strategic and campaign command information systems' effectiveness, and with the enemy's reconnaissance surveillance systems, communication systems and command and control centers as the main targets, [they should] actively organize electronic jamming and anti-radiation attacks.

1. Electronic jamming

Electronic jamming is an important means {*shouduan*} of electronic attack, and it is an electromagnetic jamming measure adopted against the enemy's electronic equipment or systems; its goal is to lower the employment effectiveness of the enemy's electronic equipment or systems. The main activities in implementing electronic jamming are: first is suppressing the enemy's air defense systems. One should comprehensively implement jamming with means such as setting up high powered ground jamming stations, employing chaff-carrying aircraft to lay **[end of page 179]** down a passive jamming corridor, sending a disposable aircraft over the enemy's radar or on the ground in the vicinity, and applying onboard aircraft electronic jamming equipment; second is jamming the enemy's satellite positioning systems. Use airborne platform electronic jamming equipment and ground high-powered jamming stations to implement jamming against the enemy's GPS receivers; third is jamming the enemy's precision guidance weapons. Deploy electronic jammers in the vicinity of our important targets and overhead

the important target areas, release jamming strips {*ganrao si*}, and employ lasers and microwave weapons as well as utilizing aerostat [lighter-than-air] weapons {浮空武器 *fukong wuqi*} to implement jamming against the enemy's raiding missiles; fourth is electronic deception. When organizing the implementation of electronic deception, in accordance with the requirements of campaign deception, deceive the enemy with electronic jamming feint attacks and passive jamming and organize campaign electromagnetic creation of circumstances/momentum {战役电磁造势 *zhanyi dianci zaoshi*} to confuse and move the enemy {迷惑调动敌人 *mihuo diaodong diren*}; and conduct this together with deception activities such as campaign camouflage and campaign feints.

The joint campaign command and his command organ should, in accordance with the electronic jamming capabilities of each operational group, adopt the method of combining separation by targets {*qufen mubiao*} and partitioning by areas-zones {*huafen quyu*} and correctly delegate the jamming missions; flexibly apply a variety of jamming modes such as active or passive jamming, selective {瞄准式 *miaozhun shi*} jamming or barrage {*zuse shi*} jamming and strive to achieve optimum jamming results; concentrate the use of jamming strengths in the important phases, main direction and key point areas, and implement a complete electronic jamming with key points at critical time occasions against the vital site {*yaohai*} electronic targets of the enemy's information systems, and thus weakening the integrated-whole effectiveness of their electronic information systems.

2. Anti-radiation attack {*fanfushe gongji*}

Anti-radiation attack is a type of IO attack form {*xingshi*} that employs anti-radiation weapons (munitions) and utilizes the electromagnetic waves emitted by the enemy's electronic equipment to track its signals and automatically seek the target and destroy it. Currently, there are mainly two types of anti-radiation weapons: anti-radiation missiles and anti-radiation unmanned aircraft. First is anti-radiation missile attack. The anti-radiation missile is an important information attack means in the future for the PLA's IO to attack the enemy's radars and screen our air penetration force-strengths. For aircraft carrying anti-radiation missiles, one normally dispatches attack aircraft {*gongji ji*}, uses unmanned aircraft to lure the enemy's radars to switch on, and then subsequently measure the enemy's radar target parameters, **[end of page 180]**, launch the anti-radiation missiles and destroy the enemy's radars in the direction of our attack so as to open up a safety air corridor for our attack formations {*gongji biandui*}. They [aircraft carrying anti-radiation missiles] can accompany the attack formation {*gongji biandui*}, together carry out penetration missions and in destroy in real-time the radar targets that constitute as threats against our air attack formation. Second is the anti-radiation unmanned aircraft attack. The anti-radiation [emanation] unmanned vehicle is a type of unmanned aircraft which utilizes the enemy's electromagnetic emanation signals as its guidance signal, tracks and destroys its emanation source. After the anti-radiation unmanned aircraft is launched, the ground control station remote-controls the unmanned aerial vehicle to fly towards the designated route; then in accordance with the pre-programmed flight to the

enemy's radar positions, it will orbit overhead and lure the enemy's radars to switch on; the search device will measure-analyze and identify the enemy's radar signal, track and destroy the enemy's radar. If, during the attack process, the enemy radar uses "silent" tactics to counter the anti-radiation unmanned aerial vehicle's attack, the unmanned aerial vehicle will resume an orbiting flight to await the time-opportunity to re-attack.

The joint campaign commander and his command organ, during the course of seizing joint campaign information dominance, command of the air or command of the sea operational activities and the campaign, they should allocate in a unified manner the employment of the anti-radiation strengths within the joint campaign task-organization and thoroughly organize the anti-radiation attack activities.

(2) Network attack

Network attack refers to the various measures and means of utilizing human designed special computer programs and computer viruses to weaken, disrupt or destroy the enemy's computer network systems or lower their operating effectiveness. For this, one mainly uses computer network infiltration means and computer virus attack means to transmit to the enemy false information, issue false orders, modify the enemy's operational documents and data, and harass their operational command. Firstly, implement computer infiltration attack {*jisuanji shentou gongji*}. One should, in accordance with higher level intent and the operational missions, organize the implementation of uninterrupted surveillance against the target networks; promptly discover the holes and fragile links that utilize the enemy network operating systems, network protocols, application software and management operations as well as [discover] utilize the inter-connection quality of a wide area network and the unbalanced quality of security protection level development; comprehensively apply techniques such as networking, computers, encryption decoding, signals analysis and protocol decoding; adopt modes such as forced penetration or looped infiltration; break through security protection mechanisms such as firewalls, gateways, encrypted authentications; and gain user rights and control privileges against target networks so as to open up passageways for subsequent attacks. Second is implementing network deception harassment. One should, in accordance with higher level intent and the operational missions, utilize the user rights and control privileges one has already grasped for the enemy's networks, harass the identification authentication mechanisms of their networks, modify their stored secret information, disrupt the integrity and accuracy of their information, interfere with the normal operations of their information systems, issue false situation, false data and false instructions at the right times, and influence and misdirect their command decision-making and operational activities. Third is implementing disruptive to paralysis attacks. One should, in accordance with higher level intent and the operational missions, apply modes such as information obstruction, virus insertion, send electronic mail bombs; conduct attacks against the enemy's networks; expend and disrupt the enemy's network resources; lower the operating effectiveness of their systems; and cause them to not be able to operate normally and even to be paralyzed. The joint campaign commander and his command organ should, in accordance with the needs-requirements of the joint

campaign's overall situation, actively organize and perform adjusting-coordination for the associated network attack strengths of the armed forces and local areas, and draw support from the nation's integrated information sources to implement attacks against the important civilian network systems that are involved in operations and hold together war potential, and thus weakening the enemy's war potential.

The joint campaign command and his command organ must tightly center on the campaign intention, and with enemy's command, control, communications, intelligence, reconnaissance and surveillance systems and civilian critical information network as the main attack targets, fully utilize the holes and fragile links within the enemy's network systems, actively organize activities such as infiltration attacks, deception harassment attacks and disruptive to paralysis attacks.

(3) Special information warfare weapons attack

In special information warfare weapons attack, this is mainly using direction finding capable weapons, electromagnetic pulse weapons and electrical network weapons to implement information attacks against the enemy. Direction finding weapon attack is mainly using direction finding weapons to blind or damage the sensors **[end of page 182]** of the enemy's electro-optical systems, and interfere with the enemy's satellite system {*xingti*}, on-satellite equipment, other information systems and main battle weapon platforms with key points and with options. The electromagnetic pulse weapon is mainly using the electromagnetic pulse weapon to implement "soft" and "hard" destruction against the enemy's electronic equipment and their personnel so as to cause them to lose operational effectiveness. The electrical network weapon is mainly using the electrical network attack weapons to disrupt the enemy's electrical facilities and electrical supply systems associated with operations.

The joint campaign commander and his command organ should fully bring into play the superior merits of special information operational weapons, and in accordance with the different situations of the targets needing to be attacked, they should flexibly apply new concept information warfare weapons against the enemy's information systems and implement attacks against their operational platforms.

(4) Psychological attack

Psychological attack is an important means of information attack. Within joint campaign IO, one must fully apply "soft-strike" and "hard-strike" means to implement psychological attacks against the enemy so as to create tremendous shock in the enemy psychologically, to put them into a state of fear for a long period of time and to achieve the goal of victory without battle. The important means for implementing psychological attack against the enemy are: first is organizing the implementation of public opinion propagation {*yulun xuanchuan*}. Regardless of whether it is before the war or during, one must fully utilize vehicles such as leaflets, pictures, broadcasts, television, computer networks, broadcasts [sic], television [sic], audiovisual periodicals {*yinxiang baokan*},

internet, etc., adopt modes such as afloat on the sea, aerial release, battlefield frontline propaganda, and implement psychological intimidation, psychological leading {*xinli youdao*} so as to shake the enemy military's hearts, collapse their morale, divide their antagonistic momentum {*didui shili*}, and strive for the hearts of the enemy's civilians. Second is applying psychological warfare weapons and implementing psychological attacks against the enemy. One can, through the use of special psychological warfare weapons such as a noise simulator {*zaosheng fangzhenqi*}, electronic whistles {*diazni xiaojiaoqi*}, thinking control weapons {*siwei kongzhi wuqi*}, and virtual reality means, etc., attack and intimidate the enemy, cause the enemy's military and people to create psychological fear or various delusions {*huanjue*} and thus shake their will for war and lower their operational capabilities. Apply hologram image weapons or laser dazzler weapons, in accordance with the needs-requirements of the operational reality, project strange images towards the enemy to cause their personnel to create delusions and psychologically create a disturbance for the enemy. Creating psychological burden to the enemy's operational personnel will generate dread **[end of page 183]** of their own safety and affect their observations, aiming and attacks. Third is employing aerostat [lighter than air] weapons {*fukong wuqi*} to implement psychological attack against the enemy. Aerostat weapons are lighter-than-air weapons such as balloons and kites and installing a delivery or dispensing device {传递布撒 *chuandi busa*} and noise-making equipment {*yinxiang qicai*} and dispense psychological warfare propaganda products so as to conduct psychological intimidation against the enemy. Employ high tech means to control the altitudes, directions and dispensing time-opportunities of the aerostat dispensing equipment will gain even better psychological warfare attack results.

The joint campaign commander and his command organ should, on the basis of the campaign intention, apply means such as public opinion propaganda and psychological warfare weapons to implement attacks against the enemy and by confusing the enemy's command and decision-making, collapse the morale of their soldiers and shake their will to make war.

(5) Firepower strike and special disruption

Implementing firepower strikes against the enemy's electronic information systems is the most thorough method for destroying the enemy's information systems, and it is an important means of information attack. The joint campaign commander and his command organ should, on the basis of needs-requirements of the realities of the campaign course, at the right time organize the missile units, aviation force units, ship units, long range artillery force-strengths, especially the precision strike force-strengths, and implement sudden, fierce and accurate strikes against the command and control centers, communication hubs and radar stations of the enemy's information systems, their bases, radar stations for reconnaissance intelligence and electronic targets such as their important intelligence information reconnaissance systems and computer network nodes as well as destroy and disrupt the vital site parts and critical nodes of the enemy's strategic and campaign information systems. The special disruption against the enemy's information systems should, on the basis of the campaign information operational plan,

dispatch special operations units via modes such as insertion, infiltration and air landing to enter the enemy's in-depth areas and implement raids against the information system vital site targets and critical nodes of the enemy's command centers, communication hubs, reconnaissance intelligence bases (positions) radar stations and network centers, striving to paralyze the enemy's information systems.

(6) Electronic deception

The joint campaign command and command organ should, on the basis of the campaign IO plan, organize electronic deception activities in a unified manner, synthetically apply dissemination of false electromagnetic information **[end of page 184]**, set-up of false electronic targets, implementation of electronic feints as well as adoption of electronic camouflage measures, and in combination with measures such as force-strength feints, firepower demonstrations, natural and man-made camouflaging, conceal our campaign intention and activities, deceive and confuse the enemy, thus causing the enemy's mistakes in judgment and lead them to mistakes in their activities.

III. Requirements of information attack…185

Information attack means are complex and diverse, and the sustained quality, integrated-whole quality and time effectiveness quality requirements of operational activities are high, so organizing command is complex and its effects on the operational overall situation are great. When implementing information attack, one should grasp the following issues:

(1) Concealed and sudden, and subdue the enemy at first opportunity

With concealed and sudden information attack, one can strike at the enemy so they cannot react in time and cause them to sink into chaos and thus lose initiative in the information domain. Therefore, one must tightly center on the campaign intention and during the critical time occasions of the campaign, concentrate various information attack strengths to suddenly initiate attacks against the enemy to cause the enemy to be too surprised to defend. One must, on the basis of the situation of the enemy's electronic targets, flexibly grasp the time-opportunity of attack, and upon discovering the enemy's fire control, guidance radars, GPS systems and the enemy's important command communication networks, one should not lose any time-opportunity to implement information attacks; [one must] strive to paralyze the enemy's electronic information systems via pre-emptive attacks; one must subdue the enemy at first opportunity via one's own active information attack activities and contain the enemy's information attacks.

(2) Prioritize targets, and strike vital sites

When organizing the implementation of information attack operations, one should set out from the campaign overall situation, prioritize information attack targets, separate

the types of the enemy's important electronic information targets, and put in order their threat level and priority sequence of attack during the course of operations. Normally, one should make the critical nodes of the enemy's electronic information systems (networks) having major effects on campaign activities the first targets of attack. As soon as these electronic information targets are destroyed, disrupted and suppressed, the enemy forces in our main operational direction will certainly lose control and this will create conditions for the PLA to seize campaign victory. In a future joint campaign, the enemy's equipment will have high value electronic information systems **[end of page 185]** such as GPS systems, advanced alert radar systems, guidance radars in a missile grouping {*daodan qun*}, infrared detection systems, communication systems, etc., and once they are destroyed or disrupted by us, they will be difficult to restore in a short time period. Therefore, once we correctly select the enemy's electronic targets, we must immediately organize our various information attack strengths to focus on the fragile links of the enemy's electronic information systems and the important nodes of their weapon control and guidance systems and implement fierce strikes so as to be able to maximally weaken and disrupt the effectiveness of the enemy's electronic information systems.

(3) Unified command, and integrated-whole operations

In a joint campaign, the enemy's IO strengths are strong and our weak, and the enemy will fully utilize various information platforms from space-based, air-based, sea-based, and land-based three-dimensional momentum-disposition to implement near-real time information support. Our information attack strengths are multi-elemented and each information attack weapon has its own merits, so only relying on a given strength or depending on a single means cannot implement effective information attack against the enemy. This requires that the PLA must implement unified command and adjusting-coordination, organically combine together a variety of information attack means, constitute a mutually compatible and functionally complementary omni-directional, multi-layered and multi-frequency band information attack system {*xitong*}, enable the operational activities of various force strengths and weaponry to mutually gain each other's merits and remedy their shortcomings, form a composite strength, and thus form an information attack strength *tixi* system that counters the enemy's electronic information system of different layers, different directions and different frequency bands so as to elevate our integrated-whole information attack capability.

Section 3: Information Defense Activities…186

Information defense activities are the synthesized protection measures and activities adopted under a unified plan and to lower the enemy's information reconnaissance and information attack results, safeguard {*baozhang*} one's own information system to bring into play one's normal effectiveness and operational information security. **[End of page 186]**

I. Information defense missions…187

The main missions of information defense are: organize anti-electronic reconnaissance, anti-electronic jamming, anti-stealth and anti-radiation destruction activities, and ensure the stable operations and of our electronic information systems and the normal bringing into play of their working effectiveness; synthetically apply various means, oppose the strikes of the enemy's firepower against our information systems, and ensure the safety of our information systems; organize the protection of our computer networks, and prevent the enemy from implementing "hacker" intrusions and virus attacks; adopt integrated measures of counter stealing of secrets, defend against leaking of secrets and defense against divulging of secrets, and ensure the maintaining of secrecy of our information security; organize battlefield electromagnetic management-control, and ensure excellent electromagnetic order on the battlefield; and organize psychological protection activities.

II. Information defense activities…187

Information defense activities must be organized and implemented with information system protection {*xinxi xitong fanghu*}, information security {*xinxi anquan baomi*}, defending against enemy psychological attacks {*fang di xinli gongji*}, and defending against special information warfare weapon attacks {*fang teshu xinxizhan wuqi gongji*} as the key points.

(1) Information system protection {*xinxi xitong fanghu*}

The joint campaign commander and his command organ should, with communication, radar and computer networks as the key points and with command centers, communication hubs, radar station, and computer network nodes as the main objectives, strictly organize the protection activities such as counter-enemy information reconnaissance, counter-enemy electronic jamming, defending against the enemy utilizing computer networks to implement information attack and counter-enemy destruction and disruption against our information systems, and ensure the campaign system's safe and stable operations.

1. Counter enemy information reconnaissance

In a future joint campaign, the enemy will apply a multi-dimensional electronic reconnaissance *tixi* system that is in all domains, in multiple layers and in all directions and implement un-interrupted reconnaissance against our electronic information systems. Consequently, we must adopt active anti-reconnaissance measures, lower the probabilities of the enemy's reconnaissance detection and tracking surveillance, cause the enemy to have difficulty with organizing effective electronic jamming, computer network attack and firepower destruct activities. First is anti-communication reconnaissance. One should, **[end of page 187]** with radio communications and enciphered communications in the lead, control the use of radio communications, adopt low acquisition probability {*di*

jiehuo gailyu} communication technology, mix together the use of a variety of communication means, and at the appropriate time, start using new model communication equipment; restrict clear enciphered and in-the-clear communications, and control communications contact times and communication quantities; strengthen management of communication encryption codes and encryption machines, strictly control allocation and use of encryption codes according to stipulation, at the right times change encryption codes and encryption keys, prevent occurrence of leaks in terms of links such as encryption key input {*miyao zhuru*}, distribution {*fenpei*} and changing {*genghuan*}. Second is counter-electronic reconnaissance. One should adopt tactical measures and technical means such as dispersing and concealing the deployment of electronic equipment, implementing electronic camouflage, electronic feints, controlling electromagnetic emanations, flexibly alternating {*linghuo bianhuan*} the employment laws of electronic equipment {*dianzi shebie de shiyong guilyu*}, and jamming and disrupting the enemy's electronic reconnaissance equipment, and decrease the enemy's electronic reconnaissance results. Third is counter-radar reconnaissance. Use the new radar technology *tizhi* system {*xin de leida jishu tizhi*}, low sidelobe antenna {低旁瓣天线 *di pangban tianxian*} and complex structure radar signals, strictly control radar signal emissions and assign mobile antennas, etc. Fourth is anti-radar network reconnaissance. One should carry out physical isolation of important military special-use networks from public networks; strengthen protection of network nodes; be strict with network systems, personnel and employment management; adopt security protection technical measures such as information encryption, [user] identification, firewall and leak-prevention, and prevent the enemy from implementing reconnaissance, acquisition and deleting-modifying our network structure, data and information contents; adopt measures such as setting up traps {设置陷阱 *shezhi xianjing*}, trace tracking {痕迹追踪 *henji zhuizong*} and virus attacks, and implement information deception or disruption against the enemy's network reconnaissance systems. Five is counter-objective reconnaissance {*fan mubiao zhencha*}. One should adopt the methods of dispersal and camouflage, conceal our important information equipment, facilities and strengthen their engineering protection {*gongcheng fanghu*}; flexibly alternate various information systems and mobile platform locations of IO weapons; set up false targets, false emplacements {*jia zhendi*}, and confuse and deceive the enemy's target reconnaissance systems.

2. Counter-enemy electronic jamming

In a future joint campaign, the enemy will widely apply various electronic warfare means and implement high intensity full time-space electronic attack activities. For this purpose, the joint campaign commander and his command organ should focus on the characteristics of electronic jamming, and with communications resistance to jamming {*kang ganrao*} **[end of page 188]** and radar counter-jamming {*fan ganrao*} as key points, thoroughly organize counter-enemy electronic jamming activities, ensuring the normal bringing the effectiveness into play of our electronic information systems. First is radar counter-jamming {*leida fanganrao*}. One should comprehensively apply strong anti-jamming capability new *tizhi* system radars such as frequency agile {*pinlyu jiebian*} and phased array and rationally deploy radars of different characteristics so as to

scientifically organize networks; under the situation of ensuring completion of tasks, strictly control the quantities and time of switching on radars; at the right time start using and concealing radars and frequencies; adopt measures such as destroying and disrupting the enemy's radar jamming sources, and improve the anti-jamming capability of radar networks. Second is communication counter-jamming {*tongxin kang ganrao*}. One should comprehensively apply strong counter-jamming capable new *tizhi* system communication means such as frequency hopping, spread spectrum and burst communications; apply a variety of equipment such as wired and radio communications, establish complex, overlapping, looped and grid state communication networks; at the right time start using concealed, alternate stations (networks) and frequencies; implement radio communication feints; adopt measures such as destroying enemy communication jamming sources, and improve anti-jamming capability of communication systems. Third is electro-optical anti-jamming {*guangdian fan ganrao*}. Adopt multi-spectrum technology {*duo guangpu jishu*}, encryption technology {*bianma jishu*}, background and target emanation discrimination technology {*Beijing yu mubiao fushe jianbie jishu*}, imaging detection {*chengxiang tance*}, and improve the counter-jamming characteristics of electro-optical equipment; adopt a composite guidance technology such as radar guidance, infrared guidance, laser guidance and television guidance, enable it so that when one encounters certain electronic jamming, one can promptly switch to a guidance mode that is not affected and continue to guide the missile to target.

3. Defend against the enemy's network attacks

In a future joint campaign, the enemy will use methods such as "hacker" infiltration and virus attacks, utilize computer networks to steal or falsify our operational information and operational data, and to throw into disorder or disrupt our information systems. Therefore, the joint campaign commander and his command organ should focus on the characteristics of the enemy's network attacks, and in terms of technology and management, thoroughly organize defense against the enemy's network attack activities. The key points of defending against the enemy's network attacks should be placed upon the critical links of our network transmission channels, exchange centers, each class of servicing devices and user terminals, and defend with key points against the enemy's penetration and infiltration attacks, deception and confusion attacks and disruption-to-paralysis attacks. In defending against network attacks, one should physically isolate our important military special-use networks and public networks **[end of page 189]**; perfect the security inspection-management {安全监管 *anquan jianguan*} and threat evaluation mechanism {*weixie pinggu jizhi*}, establish in-depth defensive systems of network early warning {*wangluo yujing*} and security monitoring {安全检测 *anquan jiance*}, and completely strengthen network inspection-controls {网络监控 *wangluo jiankong*}; in accordance with operating procedures, use firewall and intrusion inspection tools, strictly verify each class of instructions, promptly update system versions and repair system leaks; adopt encryption means, and secure databases and transmitted information data; put priority on persisting in advance defense and improve our defensive capability for unknown and smart viruses; perfect our restoration mechanism after encountering the enemy's network attack, establish an improved emergency preliminary course of action

{*yingji yu'an*}, successfully accomplish backups of system and network information, and ensure the normal operations of our network systems.

4. Resist the enemy's physical destruct

In a future joint campaign, the enemy can adopt a variety of means such as aviation force and artillery firepower attacks {*gongji*}, cruise missile long range attacks {*tuji*}, anti-radiation missile destruction, and special unit disruption-raids, and implement paralysis-quality attacks against the critical nodes and vital site parts of our campaign information systems. Consequently, the joint campaign commander and his command organ should focus on the characteristics of the enemy's implementation of destruction and disruption against our information system targets, and with resisting the enemy's precision firepower strikes, anti-radiation destruction, new concept information warfare weapons' attacks and special [ops] disruption as the key points, they should thoroughly organize the activities for resisting the enemy's physical destruction and ensure the safety of the important targets and critical nodes of our strategic and campaign information systems. On the one hand, resist the precision firepower strikes. One should disperse and conceal the deployment of our important information system equipment and facilities, as well as implement engineering protection and camouflage; flexibly alternate the locations of information system platforms and IO weapon platforms; set up false command poses, false information facilities and emplacements; implement jamming and deception against the control systems of the enemy's precision guidance weapons; strictly organize the ground-to-air alerting and missile early warning, intercept the enemy's precision guidance weapons or launch platforms, and screen the safety of our important strategic and campaign information systems. On the other hand, resist the enemy's anti-radiation destruction. One should, on the basis of comprehensively applying measure of resisting against the enemy's precision firepower strikes, rationally disposition {*bushu*} and employ **[end of page 190]** the new *tizhi* system radars of strong anti-radiation attack capability such as passive radars {*wuyuan leida*}, dual (multiple) base radars {*shuang (duo) jidi leida*}, employ means such as anti-radiation luring and adopt means such as anti-destruction, and improve our radar networks' resistance and anti-radiation destruct capabilities.

(2) Information security and classified security {*xinxi anquan baomi*}

In a future joint campaign, the enemy has advanced information technology and network attack means so the PLA's military information security and classified security {*xinxi anquan baomi*} face severe threats. The joint campaign commander and his command organ should, over the entire course and in each domain of a campaign and with prevention of loss of classified, prevention of leaking of classified and anti-theft of classified of operational information as the key points, adopt the combination mode of administrative management {*xingzheng guanli*} and technical defense-guarding {*jishu fangfan*}, and ensure campaign operations information security. First is formulating and improving the information security and classified security preliminary course of action {*xinxi anquan baomi yu'an*}. The IO command adjusting-coordination institute must

closely cooperate with departments such as the operations, intelligence and communications, establish a foothold of dealing with the most difficult and complex situation to formulate a detailed and thorough information security and classified security course of action {*xinxi anquan baomi fang'an*}, ensure the security of core secrets {*hexin mimi*}. Second is clarifying the responsibilities and measures of information security and classified security. One must rationally divide the information classification levels, strictly control the transmission scope and modes of important information, as much as possible reduce the classified knowledge scope {知密范围 *zhimi fanwei*} of operational information and the shorten the classified knowledge time {知密时间 *zhimi shijian*}. For the important information carriers such as associated plans and orders and for the important personnel involved with classified, one must adopt strict protection and defense-guarding measures; strengthen reviews of news and communication mail, and when necessary, implement information blockade against specified areas so as to prevent divulging of secrets of the news media and communication mail such as periodicals, broadcasts and television, etc.; strengthen computer network management, strengthen internet duty {网上值勤 *wangshang zhiqin*}, and bring the PLA computer information system security protection {*wojun jisuanji xinxi xitong anquan baohu*} into the national computer information system security level management track {*guojia jisuanji xinxi xitong anquan dengji guanli guidao*}. Third is strengthening information security and classified security measures. Adopt technical means such as information encryption, controlling electromagnetic emanations and prevention of computer network infiltration, and ensure the security and classified security of campaign information during the course of transmission, use and storage; adopt tactical means such as camouflage, deception, spreading false information as well as strengthening the security guarding of core vital site departments {*hexin yaohai bumen*}, and limit the enemy from gathering our true and accurate information. At the same time, one should continuously grasp the changing situation of the enemy's **[end of page 191]** IO means and modes, promptly evaluate the results of our information security and classified security measures, and adopt with a focused quality new security and classified security measures. Fourth is fully applying information security technologies. Apply cipher technologies and implement encryption protection of the important information for operating computer networks or for the installed encryption on radio communication equipment, ensure that communications with important confidential content cannot be decoded by the enemy, and gradually form an information security and classified security *tixi* system with cipher codes as the basis. Apply electromagnetic emanation wave leak protection technology {*dianci fushebo xielou fanghu jishu*}, restrain {*yizhi*} and provide a protective screen {屏蔽 *pingbi*} for our electronic information system's electromagnetic emanations and in particular, one must make protecting computer electromagnetic leaks as a key point of protection.

(3) Defending against enemy psychological attacks {*fang di xinli gongji*}

Along with the expansion of the psychological attack domain, the intensity of attacks is becoming fiercer and the technical means of attack are becoming higher, this allows the position and role of psychological protection to become more prominent. The joint campaign command and his command organ should adopt means for organizing and

administering or measures of force {*qiangzhi cuoshi*}, and consolidate one's own psychological defense line; block or disrupt the enemy's psychological warfare dissemination channels and enable the effects of the enemy's psychological warfare to not be able to effectively generate any effects. First is to build a solid psychological defense line {*xinli fangxian*}. One must strengthen thought political education, enable the officers and men to recognize that safeguarding {*weihu*} national territorial integrity and safeguarding {*weihu*} national security and stability are the duty-bound responsibilities of the military person, enhance one's sense of awareness, sense of mission and vigilance, and improve immunity to the enemy's psychological attacks. One must use the operational guidance concept to unify the officers and men's thought and activities, and enable the officers and men to maintain from start to finish a staunchly correct political position and direction; one must educate the officers and men to maintain a tenacious combat style and fearless courage and mettle, overcome flinching at hardships and being cowardly in battle, and face danger fearlessly and not be startled at the sign of danger. At the same time, one still must educate officers and men to not listen to, not believe and not disseminate the enemy's reactionary propaganda, and to not watch or keep the enemy's propaganda products. One must optimize the ambience of the collective group, coalesce military morale, and construct a sturdy psychological defense line. One must rely on the binding force and deterrence force of law and discipline {*faji*}, and standardize the active and normal psychological protection behavior of the broad mass of officers and men; one must attach importance to law and discipline towards the support role of operations, and one must punish according to law those who violate national or military laws, and thus allow **[end of page 192]** officers and men to be aware of abiding by the law, and cultivating a psychology of submitting to the law. Second is to organize psychological attacks at the appropriate time. One must adopt means of organizing and administering or measures of force, block or disrupt the transmission channels of the enemy's psychological warfare, allow the negative effects of the enemy's psychological warfare to be able to effectively develop, and thus consolidate one's own "psychological defense line." Upon ascertaining or discovering the location and activity laws {*huodong guilyu*} of the enemy's psychological warfare institution, psychological warfare units (elements) and psychological warfare equipment, as long as the battlefield situation permits, one should quickly organize and perform adjusting coordination of the force-strengths and firepower so as to conduct strikes. One must actively perform adjusting-coordination for psychological warfare units (elements) and news media to implement public opinion attacks against the enemy. Continuously ferret out the enemy's distorted propaganda {*waiqu xuanchuan*}, coalesce military morale and popular sentiment of the people, and enhance our immunity {免疫力 *mianyili*}. Particularly, one should seize upon the issues that have greater influences on unit officers and men and that most easily confuse the people's sentiments; [one should] expound on the correctness of China's current *zhidu* systems and each concept and policy from the various perspectives of national, people's and international circumstances; ferret out the irrational attacks against us by the enemy; and allow the just quality of war to become the main current of public opinion. One must successfully accomplish the work of capturing the enemy's propaganda products, one can consult the assistance of the People's Armed Police and security departments in scattered and large-in-scope areas, and when necessary, organize relevant units to conduct spot checks and successfully accomplish the work of dispelling rumors. Third is to promptly

conduct psychological restoration {*xinli huifu*}. One must utilize operational gaps, adjust dispositions, repair and maintain fortifications, wipe clean and maintain weapons and equipment, and beautify home station environment, etc., and allow the focus of officers and men to transfer the tense state of the battlefield to real things; utilize the combat transition time-occasions to consciously arrange military-civilian joint entertainment activities, further shifting the focus of officers and men and alleviate the tense mood of the officers and men. Commanders at each level must maintain words and deeds and bearing that is cool-headed, calm, steadfast, and self-confident, use thorough analysis, scientific assessments, and superior command art, improve the confidence of subordinates to gain victory and allow the mentality [psychology] of the officers and men to trend towards stability. One must utilize all time-opportunities to conduct psychological encouragement to officers and men, use deeds of heroism and the enemy's aggressive acts to arouse the operational courage and enmity of the enemy by the officers and men. One must guide the officers and men to conduct moderation of self, control their psychological state and restore psychological stability. **[End of page 193]**

(4) Defending against special information warfare weapon attacks {*fang teshu xinxizhan wuqi gongji*}

Special {*teshu*} information warfare weapons can generate a tremendous disruptive power against electronic information systems, being the "natural enemy" of electronic information warfare systems. Therefore, we must highly value the protection from special information warfare weapons. First is the protection from electromagnetic pulse munitions attack. By implementing electromagnetic reinforcement of important electronic information systems, we place electronic information systems within the cover of an electromagnetic screen so as to prevent the strong electromagnetic pulses created from electromagnetic pulse bombs from disrupting our electronic information systems; install electromagnetic inhibiting equipment on electronic conductors entering the protective screens, and prevent electromagnetic pulses from entering the protective screens through the electronic conductors and disrupt the electronic information systems. Second is protection from high powered microwave weapon attacks. Rationally deploy circuit and equipment system screens, and reduce the coupling {耦合 *ouhe*} and interference of high powered microwave weapons on information systems; rationally design cabling and electronic circuits, and enhance the capability for resisting the attacks of high powered microwave weapons; rationally select materials and parts for information systems and improve the protection characteristics for resisting high powered microwave weapon attacks; and change working modes and working frequencies, and improve the protection capabilities against high powered microwave weapons. Third is protection against high energy laser weapon attacks. Add protective layer to target coatings, cover with protective materials, and allow it [target] to allow the heat to be carried away via its protective materials when attacked by high energy laser weapons; polish surfaces and allow the laser energy deposited on the target to be lowered as much as possible; adopt new materials and reinforce structures, and improve the resistance from destruction capability of targets; employ high density and sufficient-in-range smoke screens and water screens to implement protection of targets which can cover the

enemy's laser weapons; and to the greatest extent possible, allow the missile target tail section's infrared radiations to be asymmetrical {*buduicheng*}, and increase the degree of difficulty of laser weapon attacks.

III. Information defense requirements…194

The organizing work of information defense involves a broad range of things, has many main threads, its tasks are onerous, and it has a large influence on the overall situation of operations. When implementing information defense, the joint campaign commander and his command organ should grasp the following issues: **[end of page 194]**

(1) Unified planning {*tongyi jihua*}, and thorough organizing {*zhoumi zuzhi*}

Joint campaign information defense activities {*xingdong*} involves all units using electronic information systems; it has many operational organizational entities {*zuozhan danyuan*}, it is complex in its strength structure, it is difficult for command and control and it is strong in its specialized technologies; and only by scientifically and rationally allocating and employing the various strengths and forming an integrated-whole composite strength can one ensure the security of information and information systems over the full course of a campaign. Consequently, one must set out from the overall situation of the campaign, perform unified planning, thorough organizing, and successfully perform operations research-based planning for information defense activities. First is to perform unified formulation of the information defense plan. The joint campaign information defense plan should be drafted together by the associated departments of the joint command {联指 *lianzhi*} information operations, communications, intelligence, and classified {*jiyao*}. Second is dispersed implementation and close coordination. In accordance with the joint command information defense plan {*lianzhi xinxi fangyu jihua*}, each operational group {*zuozhan jituan*} (grouping {*qun*}), based on the general requirements {*zongti yaoqiu*}, will separately draft their own information defense plan, and accomplish linkup from top to bottom {*shangxia xianjie*}. Third is full course monitoring-control, and at the appropriate time adjustment. During the course of the entire campaign, one must strengthen the degree of real-time monitoring-control, issue information reconnaissance intelligence, gather the information defense situations, analyze the information defense postures, evaluate the defense results, at the right time adjust the information defense disposition, depending on the situation, change the means of defense, and form an effective full-course control.

(2) Synthesized application {*zonghe yunyong*}, and integrated-whole defense {*zhengti fangyu*}

During joint campaign IO, the enemy will inevitably employ a variety of information attack means and implement information attack against us in multiple dimensions of space. To this end, when organizing and implementing information defense activities, one must first focus on synthetically employing a variety of means to unfold uninterrupted confrontation against the enemy, and with active and effective

technical and tactical measures, strengthen the protection of our information systems. Secondly, one must synthetically apply a variety of strengths, establish a unified intelligence reconnaissance *tixi* system and command and coordination network, achieve interconnected sharing of intelligence, form an integrated-whole composite strength of information defense that has mutual adjusting-coordination and complementary functions, and ensure the bringing the effectiveness of our electronic information systems into play. Thirdly, one [must] fully utilize and perform unified adjusting-coordination of the information defense strengths of the civilian domain, construct an information defense *tixi* system that is military-civil as one {*junmin yiti*}, highly integrated {*gaodu jicheng*} and can cover multiple dimensions of space, **[end of page 195]** form a security mechanism {*anquan jixhi*} that shares military and civil information networks, and ensure the integrated-whole security of military information systems.

(3) Complete defense {*quanmian fangyu*}, and give prominence to key points {*tuchu zhongdian*}

During future joint campaign IO, the PLA information system {*xitong*} touches upon many units, its scope is broad, structure is complex, integrated-whole quality is strong, its sub-systems {*fen xitong*} are tightly combined, and damage to any one critical part will affect the stable operations of the entire system. Therefore, when organizing and implementing information defense activities, one must establish a foothold in the actual situation of the PLA's integrated-whole information defense capability is weaker, so not only must we successfully accomplish omni-directional {*quan fangwei*}, full time-space and complete information defense work, we must also give prominence to the important time-occasions, key-point areas and key-point targets to conduct key-point strikes. Firstly, based on the needs of each time-occasion of the campaign, give prominence to key-points of defense {*fangyu zhongidan*}. In the organizing preparations phase of the campaign, the enemy will inevitably implement information reconnaissance, direction-finding and fire strikes against us, so the key-point of information defense is to counter the enemy's reconnaissance and destruction; during the campaign implementation phase, the enemy will apply electronic jamming means and anti-radiation weapons, and implement jamming suppression and anti-radiation destruction against our electronic targets. Secondly, in terms of the means of defense, we should give prominence to electronic defense and network defense. Center on the two large missions of defending-protecting information systems and information security, ensure survival-safety {*shengcun anquan*} and effective working of our information systems by organizing electronic defense; and ensure the security {*anquan*} and maintaining secrecy {*baomi*} of our campaign information by organizing network defense. These two information defense activities must complement each other and we cannot do one and not the other. **[End of page 196; end of chapter]**

This page intentionally left blank.

Chapter 10
Adjusting-Coordination and Control of Joint Campaign Information Operations…197

Joint campaign information operations [IO] is not only the confrontation between the IO strengths of both sides, it is also the contention {角逐 *jiaozhu*} between the IO command of both sides and whether one can accomplish prompt, highly effective, stable, accurate and flexible adjusting-coordination and control directly relates to whether one is able to seize joint campaign information dominance or even campaign initiative. Therefore, on the basis of the composition of the joint campaign command institution and the specific situations of IO, one must implement effective adjusting-coordination and control of IO activities.

Section 1: Joint Campaign IO Adjusting-Coordination…197

Joint campaign IO adjusting-coordination refers to process of looking after {调理过程 *tiaoli guocheng*} aspects such as time, space, inter-relationships and activity modes of various IO strengths during IO. The structure of the joint campaign IO strength is complex, its equipment types are numerous, and its operational patterns are varied, so thorough adjusting-coordination has important significance for maintaining ordered continuity of IO activities and bringing an integrated-whole effectiveness of IO into play. For IO adjusting-coordination, what is critical is one must successfully grasp the time-opportunities, content and methods of IO adjusting-coordination. **[End of page 197]**

I. Time-opportunities of adjusting-coordination…198

IO adjusting-coordination is an uninterrupted continuous process that permeates IO command from beginning to end. Correctly grasping the adjusting-coordination time-opportunity is critical for seizing IO adjusting-coordination initiative {*zhudongquan*}. To this end, based on the senior officer's resolution and the IO plan, one must take aim at the battlefield realities, correctly grasp the time-opportunities, separate the main-secondary and greater and lesser urgencies {*qufen zhu-ci huan-ji*}, and successfully perform adjusting-coordination for unit IO activities by being thorough and reliable {*zhoumi wentuo*}, at the right times and without interruption.

On the basis of the development of joint campaign activities, grasp the time-opportunities of adjusting-coordination. IO is in the service of joint operations, and its activities must accept the constraints and effects of joint operational activities. When changes occur to joint operational activities, changes to IO activities must also occur. At that time, one must organize IO adjusting-coordination and allow IO to achieve organic complementation of joint operations. For example, when one conducts major adjustments to the operational direction, when operational missions and operational phases transition, or when reserve forces are committed into engagements, one needs to re-organize IO adjusting-coordination.

On the basis of the course of IO, successfully grasp the time-opportunity of adjusting-coordination. IO is conducted during the fierce confrontation between both sides, therefore, due to subjective or objective reasons, this brings about frequent occurrence ordered situations changing into disordered situations. For example, when an attack is foiled, the plan is thrown into chaos, IO systems suffer disruption and interference, major changes occur in the enemy situation, shifts occur to the original operational objectives or new operational objective appear, etc., this creates disorder for IO activities, so at this time, one must conduct IO adjusting-coordination.

In order to successfully grasp the time-opportunity for IO adjusting-coordination, it is critical for one to strengthen forecasting {*yuce*}, promptly discover potential imbalances or chaos, and one cannot wait until after a chaotic situation occurs and then reactively {*beidong de*} organize adjusting-coordination which will inevitably create difficulties for performing adjusting-coordination. At the same time, one must conduct in-advance planning and substantive [materialistic] preparations {*wuzhi zhunbei*}, and this is the substantive basis for achieving adjusting-coordination at the right time. If one has in-advance planning and preparations, one will not lose the time-opportunity and quickly conduct adjusting-coordination. Otherwise, it is possible to cause IO to fall into passivity [reactive] {*beidong*}. **[End of page 198]**

II. Content of adjusting-coordination…199

The content of adjusting-coordination refers to the main adjusting-coordination items of IO. From the perspective of several recent local wars, IO adjusting-coordination mainly includes the content of the following areas.

(1) Adjusting-coordination of IO strengths

In joint campaign IO, the building of IO strengths has emerged the characteristic of having multiple elements. From the perspective of participating service and arm structure, there are Army, Navy, Air Force and Second Artillery IO strengths and local IO strengths, etc. From the perspective of a layered structure, there are strategic, campaign and tactical IO strengths. From the perspective of mission nature and functional structure, there are IO command strengths, IO attack and defend strengths and IO support strengths, etc. In terms of specialty types, there are specialized IO strengths and non-specialized Io strengths, soft kill strengths and hard kill strengths, etc. In performing adjusting-coordination of IO strengths, on the basis of the IO missions of the participating units, one mainly conducts strength allocation {*diaopei*}, clarifies the operational activities of each strength and their inter-relationships so that the strength employment matches their assumed missions as well as being in adjusting-coordination with the functions that should be brought into play for each strength. Only in this manner can their superiorities complement each other and one can conduct operations with consistent adjusting-coordination {*xietiao yizhi*}.

(2) Adjusting-coordination of IO resources

IO resources refer to the material technical conditions relied to conduct IO. In performing adjusting-coordination of IO resources, one essentially conducts a rational assignment and adjustment of the various limited resources needed for IO. In performing adjusting-coordination of IO resources, one must conduct it in conformance with the principles of key-point support of the main operational direction, key-point operational activities and critical-quality operational time-occasions, and mainly perform adjusting-coordination for information support, communication network support, weapons and equipment support and technical support so as to produce a higher support benefit {*xiaoyi*} from limited IO resources through rational adjusting-coordination and deployment {*peizhi*}. Under normal situations, in addition to successfully accomplishing the adjusting-coordination of hard resources such as various information weapon systems and information networked battlefield building to include battlefield information systems, **[end of page 199]** one must also successfully accomplish adjusting-coordination of soft resources, namely, through the IO center performing unified operations research-based planning, one builds accurate, complete and reliable intelligence and command systems, at the right time sorts and arranges of all of ours and the enemy's intelligence information, continuously updating and building a dynamic state and automate updating large scale battlefield database which can provide sharing by the entire IO system.

(3) Adjusting-coordination of IO space

The IO space {*kongjian*} refer to the space {*kongjjian*} and location {*weizhi*} occupied by IO strengths. The modern IO space is a multi-dimensional battlefield space, not only is there IO on the land battlefield, there is also IO in the sea battlefield, air battlefield, electromagnetic battlefield and space battlefield. Any type of IO activity unfolds in a specific space and is centered on the general operational intention {*qitu*} and operational target. In order to allow various IO strengths to have ordered activities in their respective spaces, to not affect or interfere with each other, then one must successfully accomplish adjusting-coordination of the IO space. Normally, this is mainly to perform adjusting-coordination of the various IO strengths in their deployment of space and unfolding locations, [perform adjusting-coordination of] the deployment of activity areas-zones, activity directions, operational targets and information systems and unfolding locations, shifted routes and sites {*zhuanyi luxian he didian*}, etc.

(4) Adjusting-coordination of IO activities

The IO activity is the designation for the various attack activities, defense activities and support activities in IO. When considering the characteristics of integration of offense-defense and combining of "hard" and "soft" with a highly blending of other operational activities, and in order to allow the various IO activities to supplement and complement each other, one must strengthen the adjusting-coordination of IO activities. Under normal situations, the is mainly to successfully accomplish the complementation of the adjusting-coordination between IO activities and joint operational activities; the

complementation of the adjusting-coordination between information attack and information defense; the complementation of the adjusting-coordination between IO and information support; and the complementation of the adjusting-coordination between various information attack operational activities and means, etc. **[End of page 200]**

(5) Adjusting-coordination of IO time

IO time refers to the expended time during the course of IO. Any given IO activity demonstrates a specified course of time, so in order to allow for various IO activities to achieve excellent complementation in terms of time, one must strengthen adjusting-coordination of operational time. Normally, this is mainly to perform adjusting-coordination for the start time, operational tempo, operational phase linking and transitions of each IO activity. Only through close complementation in terms of time can one enable the various operational activities to keep in step and form a composite strength.

III. Methods of adjusting-coordination…201

The scientific and rational adjusting-coordination method is a specific embodiment of operational command art, and it is an important factor affecting the effectiveness of adjusting-coordination. Based on the characteristics of IO and the requirements on IO command, one can adopt the following adjusting-coordination methods in IO.

(1) Consultative adjusting-coordination method

Consultative adjusting-coordination {会商协调 *huishang xietiao*} is the adjusting-coordination conducted by each side within the operational task-organization of operations undertaking IO missions via consultation to achieve consensus for the associated adjusting-coordination items of coordinated operations. In consultative adjusting-coordination, because one normally must fully listen to the adjusting-coordination recommendations of each side and undergo the approval of each side, this kind of adjusting-coordination is specific and precise, the adjusting-coordination is easily accepted by each side and in execution, it readily obtains the active complementation with initiative of each side; the quality of its adjusting-coordination is high and its results good, but because of more expenditure of time for conducting consultative adjusting-coordination, it is normally used pre-battle for all-services and arms coordinated operations with more preparation time. The form of consultative adjusting-coordination can be sending representatives to the consultative conference, or it can be conducting a communications consultation. The results of consultative adjusting-coordination is normally issued to the associated organizational-units of coordination in the form of a coordination plan {*xietong jihua*} and then executed.

(2) Instruction adjusting-coordination method

Instruction adjusting-coordination {*zhiling xietiao*} is adjusting-coordination conducted through directly issuing coordination instructions {*xietong zhishi*}. During the course of IO implementation, when an imbalanced situation appears suddenly, time is tense and missions are weighty, one cannot first conduct adjusting-coordination through consultation, one must organize the adjusting-coordination method via prompt issuance of coordination instructions **[end of page 201]**. Ordinarily, this is established on the basis of the coordination plan and having preparations pre-battle for the situation of coordination imbalance {*xietong shitiao*}. This has higher requirements on the adjusting-coordination institution and communication support.

(3) Communicated adjusting-coordination method

Communicated adjusting-coordination {*goutong xietiao*} mainly refers to the adjusting-coordination conducted via prompt situations communicated with higher level and friendly IO units. Because there isn't a subordination relationship between friendly and higher level IO units, for the adjusting-coordination of IO between them, one can only achieve close complementation and adjusting-coordination through communicating of regular-quality information. To this end, one must promptly issue bulletins on the relevant situations of one's own unit's IO to friendly and support {*zhiyuan*} units. At the same time, one must also, as necessary, comprehend the IO situations of the friendly and support {*zhiyuan*} units, and on the basis of the situation, put forth the coordination requirements of one's own unit as well as organize subordinate units to successfully accomplish coordination and complementation with friendly and support {*zhiyuan*} operational units.

IV. Requirements of adjusting-coordination…202

In order to successfully organize IO adjusting-coordination, one should resolutely put into effect the instructions of the higher level and senior officer, focus on the overall situation, seize upon the main contradiction, and actively and reliably conduct it. During the course of specifically organizing [adjusting-coordination], one should pay attention to accomplish the following points: first is to resolutely put into effect higher level and senior officer instructions. Adjusting-coordination is the specific measure {*juti jucuo*} for putting into effect and carrying out the senior officer's resolution, and IO adjusting-coordination must be conducted on the basis of the IO plan and higher level and senior officer instructions. Second is attaching importance to the integrated-whole quality of adjusting-coordination. The so-called integrated-whole quality of adjusting-coordination refers to when the IO departments are organizing adjusting-coordination, they must focus on the overall situation, not only must they grasp the complete integrity of adjusting-coordination content, they also must allow for an organic combination of the various aspects of adjusting-coordination content, and thus truly reflect the integrated-whole might of the all-services and arms joint IO. Third is strengthening the foresight quality of adjusting-coordination. For the adjusting-coordination of all-services and arms IO,

because going from the joint campaign IO departments to the services and arms command post's IO departments, and then again going to the informationized weapon platforms of the first-tier IO units require a period of time, thus operational adjusting-coordination must be established on the basis of scientifically foreseeing the situations of the joint **[end of page 202]** operations battlefield. Otherwise, if we wait until the battlefield situation becomes extremely urgent before performing adjusting-coordination for the activities of each IO unit, we certainly cannot catch up to the changes of the battlefield situation and lose the significance of performing adjusting-coordination. Fourth is to grasp the layered quality of adjusting-coordination. The layered quality of adjusting-coordination refers to clarifying and ensuring the adjusting-coordination duties-responsibilities and successfully grasping the limits of authority {*quanxian*}. The adjusting-coordination belonging to the scope of one's own level of adjusting-coordination duties-responsibilities must be thoroughly implemented; the adjusting-coordination content belonging to the scope of subordinate level duties-responsibilities must be left for lower levels to implement so as to avoid too many orders going out, units uncertain what to do and resulting in confusion of activities. Fifth is seizing upon the main contradiction, and actively and reliably conducting [adjusting-coordination]. For IO adjusting-coordination, one must tightly seize upon the main contradiction, grasp the operational center of gravity, clearly separate the main-secondary and what is urgent and not urgent, conduct unified operations research-based planning and arranging {*tongchou anpai*}, and to the greatest extent bring into play the role of adjusting-coordination. One must promptly discover and grasp non-adjusting-coordination factors, conduct analysis and research, clearly separate the issues of main-secondary, and conduct assessments for the aftermath {*houguo*} and degree of danger {*weihai chengdu*}; promptly ascertain the adjusting-coordination targets and adjusting-coordination method; rigorously organize adjusting-coordination, strengthen information feedback, and ensure that the adjusting-coordination work is conducted according to adjusting-coordination objectives {*mubiao*} and courses of action {*fang'an*}.

Section 2: Joint Campaign IO Control…203

IO command and control refers to, during the course of IO, the commander and his command organ, in order to achieve the pre-designated operational objectives and through the series of activities such as issuing instructions, tracking feedback, posture analysis and regulating-controlling and error correction, promptly correcting the appearance of deviations and imbalances in IO activities and allowing various IO strengths and IO activities to develop according to the direction of pre-designated objectives and to ultimately complete one's IO missions.

I. The method of control…203

(1) Objective control method {*mubiao kongzhi fa*}

The objective control method is control conducted with objectives [targets] and missions determined by IO **[end of page 203]** as the criteria {*zhibiao*}, and it is a type of

method for controlling the results of action {*xingwei jieguo*}. Its characteristics are: use a specific objective or achieved posture to guide {*yindao*} IO activities, and ultimately eliminate the gap between a current activity state {*xianshi xingdong zhuangtai*} and the objective [target] state {*mubiao zhuangtai*}.

There is a large amount of flexibility in using the objective control method, whereby the object being controlled may, under the situation of determining the objective, fully bring into play one's own subjective dynamic quality and on one's own initiative select activity measures. This type of control method not only can [be used to] reflect the command art of those in command through selecting of controls, it can also [be used to] inspect the level of command of subordinate-levels through the object being controlled. The objective control method has lower requirements for communications contact, and even in the situation of losing communications contact, a unit can still be placed in a control state without the appearance of too much confusion, but it does require for the object of control to possess a higher quality and command ability. The shortcomings of the objective control method are: it is not easy for those in command to control the activities of the object of command, or in other words, under this type of control method, those in command have a weaker ad hoc control over the object of command; it does not facilitate the coordinated activities between the objects of command. Therefore, normally, adopt this type of control method in the situations when one does not need to restrict the activities of the command object or when there is no way to restrict the command object.

To use the objective control method, one first resolutely implements control based on set objectives {*jiding mubiao*}. After IO activities begin, the commander must resolutely implement control of objectives in accordance with the operational intention and the IO plan. When a fundamental quality change {*genbenxing bianhua*} has yet to occur in the battlefield situation, one may not rashly alter the operational objectives. Secondly, on the basis of the changing situation, promptly revise objectives {*xiuzheng mubiao*}. During the course of IO control, there is a process of uninterrupted feedback of information, {*buduan fanyi xinxi*} conducting posture analysis {*jinxing taishi fenxi*}, setting corrected resolutions {*dingxia jiupian juexin*} and implementing adjustment and control and error corrections {*shishi tiaokong jiupian*}, and if a fundamental change {*genben bianhua*} occurs in the battlefield situation, one should promptly revise the objectives based on the changed battlefield situation and implement control in accordance with the post-revision operational objective. Thirdly, rationally separate the operational objectives. The operational objectives at one's own level are tightly connected to the subordinate-level's operational objectives and with each sub-objective of operations, **[end of page 204]** the objectives must have a better measurable quality, and when necessary, one may attach a specific restrictive condition to an operational sub-objective. Fourthly, maintain an excellent adjusting-coordination relationship between each object of control. One must determine the inter-connections and restrictive conditions between the operational sub-objectives; one should establish an excellent adjusting-coordination mechanism between the objects of control, allowing one to be able to adapt to the developing changes in the battlefield situations, at any time adjusting the coordination relationships, and ensuring ordered uninterrupted coordination actions.

(2) Plan control method

The plan control method {*jihua kongzhi fangfa*} is a method of conducting control for the course of IO activities with the operational plan as its basis. It is a control method that is a combination of feedback {*fankui*} and forward feedback {*qiankui*}. It is the most common and practical method used in IO control. Its characteristic is to use the pace of achieving objectives to restrict the activities of the object of control.

The IO plan control method possesses the following merits: first is its task requirements are clear, it has unified control standards, and it facilitates discovering and correcting deviations. Second is it does not have too high of requirements on communications contact, and under complex and difficult situations, one can also conduct coordinated operations. Third is it can fairly successfully bring into play the command role of those in command and avoid each object of command going their own way. The weak points of the plan control method are: it lacks in resisting interference and adapting to change; when one encounters the occasional situation outside of given plans, the plan may be thrown into confusion and influence the control results; so one must re-formulate the plan and establish a new plan control, and sometimes, one cannot accomplish this in time.

Based on the differences of the IO phases, there should be differences in employment of the IO plan control method. In the first phase of operations, because there is a longer period of time to comprehend the opponent's initial situation and conduct calculations and preparations, the effects of various situations on the plan aren't great, so one normally adopts somewhat stricter plan control. As operations develop, because situations that were not predicted beforehand increase, and because there isn't ample time to be used to revise a plan or formulate a new plan, so one can only adopt an outline plan control **[***gailue de jihua kongzhi***]** method or adopt another method to conduct control.

To use the plan control method, first, one determines the control standards of the plan {*jihua de kongzhi biaozhun*}. The IO plan should include the activity time, space, objective and tasks for the activities of each object of control as well as other content stipulated by those in command. Secondly, one grasps the activities of the control object via supervision and feedback, and compares all states one can be in with the anticipated states in the plan to find the deviations. Third, one issues correcting adjustment-control instructions on the basis of the size of the deviations and the effects on follow-on activities. The issuance of IO activity correction instructions becomes the basis for the control object's activities. Under normal situations, after the control object receives the instructions, they must strictly adhere to the detailed activities stipulated in the plan, and they must promptly report to higher levels their execution situation.

(3) Ad hoc control method

The IO ad hoc control method {*suiji kongzhi fa*} is the control method used by those in command via temporarily issued instructions to standardize and bind {*guifan and*

yueshu} the command object's activities for IO situations where deviations and activity imbalances appear. The ad hoc control method is implemented in the situations of not being able to implement objective control method or the plan method, and it is control conducted without a plan or outside of a plan. The greatest superiorities of the ad hoc control method are the period of control adjusting-coordination is short and its response time is fast. Especially when the situation changes suddenly, it facilitates the commander to quickly react in controlling subordinate units (elements). However, this control method has a high requirement on intelligence and communications contact, it requires those in command to have higher ability for rapid response and as decisive as called upon. The ad hoc control method is control that is ordinarily conducted under the conditions of not having a plan for an event beforehand or if the plan is not prepared and communications contact also has ample support {*baozhang*}, and significant changes or imbalances appear in the battlefield situation. It requires those in command to completely, promptly and specifically have mastery of information or those in command will not be able to issue correct orders and the command objects will be placed in a loss of control state. Moreover, the ad hoc control method also requires those in command to maintain uninterrupted connectivity with the objects of command. **[End of page 206]**

After issuing the control order, the commander should, on the basis of the supervision and feedback situations, promptly inspect the object of command's execution of the order situation, and if he discovers deviations not conforming to the commander's analysis and assessment conclusion, he will issue corrective orders depending on the situation.

To use the ad hoc control method, first, one employs different control methods based on different situations. The battlefield situations of different operational activities, operational methods and operational phases are different, and the command support conditions are also different, so this requires one to employ different control methods. For example, in the initial phase of IO, because the time to plan and organize operations is abundant, the formulated plans are also fairly thorough and specific, communication support is also strong, and as a result, one can use the plan control method more. Secondly, one draws on the strong points of others to offset one's weaknesses and bring into play the merits of different methods. Using many methods to implement control benefits the merits of bringing different control methods into play, facilitates drawing on the strong points of others to offset one's weaknesses, and achieves greater IO results. For example, in IO of the main direction and key point targets, one can conduct control on the basis of the formulated in-advance plan and bring into play the might of integrated-whole operations. But when significant changes occur to the battlefield situation or if the IO deviates from target, when communication support is basically unimpeded, one can additionally implement ad hoc control, promptly eliminate deviations and errors from operational activities, reduce losses and ensure the realization of the operational goal. Thirdly, one synthetically applies in a overlapping fashion a variety of methods. Objective control is suitable for control of units with a stronger IO capability and facilitates cultivating and improving the independent operational capability of units. Plan control is suitable for IO of a larger scale, easily brings into play the command art of a commander, and achieves a commander's resolution. When the

battlefield situation changes are especially rapid and the battle situation is especially complex, one frequently overlaps and synthetically applies a variety of control methods so as to achieve effective control of IO.

II. Requirements of control…207

In IO control, the basic criteria must be to achieve the operational goal, so focus on the operational activity characteristics, and on the basis of the actual needs-requirements of operational command, promptly and resolutely implement it. **[End of page 207]** During specific implementation, one should pay attention to accomplish the following points:

(1) Clarify authority, and implement with division of labor

IO control is the important activity of the IO command institution at each level. During the course of control implementation, one should clarify the command authorities of the IO departments and IO unit commanders at each level. For example, [clarify] the command authority of the IO units for the higher level support {*zhiyuan*} to operations and the IO units of each service and arm, and the command authority of each commander of each phase of IO so as to facilitate the effective bringing into play of command and control effectiveness.

(2) Control at the appropriate time, pay attention to time effectiveness

The goal of IO control is to effectively master {*zhangwo*} IO strengths and allow them to perform activities in accordance with the general intent {*zongde yitu*}. Its essence is to adopt all means and measures and ensure the effectiveness of one's own command and control while simultaneously disrupting the enemy's command and control and causing their command and control systems to be paralyzed. Therefore, one must conduct control at the appropriate time and improve the time effectiveness of IO control. First, one must apply all utilizable reconnaissance means to form an as complete as possible intelligence surveillance network {*qingbao tance wang*}, establish reliable information transmission channels, and ensure the prompt collection and notification of various information. Secondly, the commanders and IO departments at each level must have a very strong independent command capability, and in particular, they must possess the capability to quickly ascertain the situations and implement correct control when the situation is critical or when the intelligence volume is insufficient. Thirdly, during the campaign preparation phase, one should formulate a thorough IO plan, anticipate a variety of situations and their corresponding activity courses of action {*xingdong fang'an*}, and establish the necessary adjusting-coordination and control mechanisms so as to establish a foundation for high quality and highly effective operational control.

(3) Set out from the overall situation, and grasp the key points

Controlling key points is the important principle for implementing effective control. In ordinary situations, the flow of information within the control system has multiple elements, the object of control has multiple factors, and the change in the system environment has multiple aspects. Therefore, the one who commands must set out from the overall situation, and while relying on the deviation signals of each area, he must tightly have a grasp on the "pivot" {*shuniu*} influencing the course of IO and the overall situation, **[end of page 208]** and strengthen the strict control of the operational critical link points {*guanjie dian*}.

In the organizing phase of IO, one must conduct a complete plan with key points for the full course of operational activities, particularly for the main operational direction, operational phases (time occasions {*shijie*}) and operational activities. One must as much as possible consider the various difficult situations {*kunnan jumian*}, accomplish ample demonstrations, make thorough arrangements, and allow relevant personnel to be familiar with these beforehand. During the IO implementation phase, one must fully utilize all utilizable intelligence gathering means to implement complete reconnaissance and surveillance with key points against the enemy, and in particular, one must pay attention to the reconnaissance of situations such as the locations of the enemy's high-powered jamming equipment, precision guidance weapon systems, command and control hubs, the enemy's battlefield information networks and their main nodes, etc. Additionally, one must issue prompt bulletins on associated situations to all subordinate units (elements), so as to facilitate combining this with the current enemy situation and pre-accomplish preparations for potential developments of future situations. When unexpected and difficult situations {*jumian*} appear, one should, on the basis of complete analysis of the situation, seize upon the key points, quickly adjust dispositions, and from start to finish maintain effective control of the main operational units and main operational activities.

(4) Appropriate degree of control, and be unified but not to death {统而不死 *tong'er busi*}

The object being controlled {施控对象 *shikong duixiang*} in IO is a dynamic-state system, its control missions are in maintaining this system or in the stability and order of organizing, and this allows it to be brimming with vigor. The crux for accomplishing being unified but not to death and being full of vigor but not in chaos {*huo'er buluan*} refers to conducting control within an appropriate level.

To accomplish an appropriate degree of IO control, first, one must adhere to the basic tenet of control of successfully accomplishing the affairs belonging within the scope of one's own duties-responsibilities, and not to monopolize power {大包大揽 *dabao dalan*} and excessively interfere on the affairs belonging in the scope of the object of control. Secondly, one must fully bring into play the role of vertical and lateral control systems {*chuizhi he shuiping kongzhi xitong*} and conduct control function by function, with layers and with scope. Thirdly, one must successfully resolve the contradictions

between effective control and maintaining the vigor of the object of control, and allow control to have a specified elasticity and dimension. **[End of page 209]**

This page intentionally left blank.

Chapter 11
Operational Support {*zuozhan baozhang*} for Joint Campaign Information Operations…210

Operational support for joint campaign information operations (IO) is the general term for the various support measures adopted in order to smoothly carry out IO missions {*xinxi zuozhan renwu*}, and for their corresponding activity {*huodong*}. [Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.] It is an important factor {*yinsu*} in composing and maintaining the combat capability {*zhandou nengli*} of the IO units {*budui*}, and is an important component {*zucheng bufen*} of joint campaign operational support, one which penetrates through the entire process of joint campaign IO activities {*xingdong*}. Its basic missions are to support the joint campaign commander [JCC] {*lianhe zhanyi zhihuiyuan*} in timely setting the IO resolution {*dingxia xinxi zuozhan juexin*}, to support the JCC in implementing effective command of the IO units, and to support the smooth conduct of joint campaign IO activities.

Section 1: The Content of IO Support…210

Operational support for joint campaign IO generally is specifically {*juti*} implemented by the operations, communication {*tongxin*}, cryptography {*jiyao*}, engineering, surveying and mapping {*cehui*}, meteorology {*qixiang*}, and hydrology {*shuiwen*} departments, adjusted-coordinated {*xietiao*} by the IO command institution {*zhihui jigou*}. It mainly includes the following content: target {*mubiao*} support; communication support; cryptographic support; engineering support; electromagnetic [EM] spectrum management {*dianci pinpu guanli*}; nuclear, chemical, and biological [NBC] protection {*he hua sheng fanghu*}; position warning and defense {*zhendi jingjie yu fangwei*}; surveying and mapping support; meteorological and hydrological support; and battlefield management. **[end of page 210]**

I. Target support…211

Joint campaign IO target support signifies carrying out collection, arrangement {*zhengli*}, and processing of information targets, such as the enemy's main information systems {*xinxi xitong*} and information offense {*xinxi jingong*} weapons and equipment {*wuqi zhuangbei*} acquired by IO reconnaissance {*xinxi zuozhan zhencha*}, and thus determining the information targets' classes {*zhonglei*}, degree of importance {*zhongyaoxing chengdu*}, and threat level {*weixie dengji*}, as well as means and measures for attack. It is implemented under the responsibility of the joint campaign command's {*lianhe zhanyi zhihuibu*} IO reconnaissance and intelligence department {*zhencha qingbao bumen*}, as well as under that of IO groups (groupings) {*jituan (qun)*} and of the IO grouping reconnaissance and intelligence departments of all services and arms {*ge junbingzhong*}. Joint campaign IO target support is the basis of and a prerequisite {*qianti*} for effectively implementing information offense and information

defense {*xinxi fangyu*}, and is an important assurance of seizing and maintaining local information dominance {*jubu zhixinxiquan*}.

Target information collection {*huizong*} indicates that the IO department carries out centralized special collection {*jizhong guikou huizong*} of all-source {*gezhong laiyuan*} target information, and carries out its sorting and registration {*fenlei dengji*}. This includes the following: target information downward released by the higher levels {*shangji xiafa*}, target information acquired by various reconnaissance means {*zhencha shouduan*}, and target information provided by friendly neighbors {*youlin*} and by locales {*difang*}, as well as target information extracted from open sources {*gongkai ziliao*}.

Target information arrangement means conducting analysis and research {*fenxi yanjiu*} on the acquired target information, reaching conclusions, and arranging them into written form, to facilitate further processing or briefing and distribution {*fenfa*}.

Target information processing means carrying out reporting or briefing of well-arranged target information, based on the needs and requirements {*xuyao*} of IO and the nature of the target information. For strategic-quality target information {*zhanluexing mubiao xinxi*} or for target information which influences the overall situation of the campaign {*zhanyi quanju*}, the JCC should personally organize personnel to carry out the analysis and research, and do the processing. Target information which is directly correlated {*xiangguan*} to unit operational activities should be timely briefed to the units; and target information which is correlated to friendly neighbors should be timely briefed to the friendly neighbors. Target information which has not undergone validation {*zhengshi*} and also is urgent should be immediately reported, and investigated while it is being reported {*biangao biancha*}. Not firm {*buwen*} target information should be reported or briefed after it is synthesized {*zonghe*}.

II. Communication support…211

Joint campaign IO communication support indicates **[end of page 211]** the general term for the various assuring measures {*baozhengxing cuoshi*} adopted by, and corresponding activity carried out by the communication units (elements) {*tongxin bu (fen) dui*} and associated strengths in signal communication {*tongxin lianluo*} respects, in order to ensure the smooth fulfillment of IO missions. IO communication support is the basic means for supporting IO command and for adjusting-coordinating IO activities, and has important significance for assuring the rapid transmission {*chuandi*} of information, for linking the various IO strengths into an organic integrated whole, and for boosting IO effectiveness {*xiaoneng*}. Usually it is adjusted-coordinated and organized by the joint IO department and communication department. [These departments] should, based on the joint campaign communication {*zhanyi tongxin*} support plan {*jihua*} and IO command needs and requirements, and relying on the campaign communication system of systems [SoS] {*zhanyi tongxin tixi*}, exploit the subordinate (reinforcing {*jiaqiang*})

communication strengths to establish an IO intelligence, command, and coordination communication net {*qingbao, zhihui he xietong tongxin wang*}.

The main missions of communication support are as follows: to organize and establish an IO command communication net, and support the unimpeded flow of communication by the IO command institution with its subordinate IO units; to organize and establish an IO coordination communication net, and support coordination communication among all IO units, as well as between the IO units and other operational units; and to organize and establish an IO intelligence transmission net {*qingbao chuanshu wang*}, and support the unimpeded flow of IO intelligence communication. Its basic requirements {*yaoqiu*} are as follows: to synthetically [comprehensively] apply {*zonghe yunyong*} various communication means to establish a high-stability, high-communication-capacity, high-transmission-rate {*chuanshu sulyu kuai*} IO communication network which is vertically and horizontally linked up {*zongheng guantong*} and has multipath bypassing {*yuhui duolu*}, and to ensure the transmission of battlefield information in a rapid, accurate {*zhunque*}, secure {*baomi*}, and uninterrupted {*bujianduan*} manner.

The main measures are as follows: the first is reliance on the joint campaign integrated communication net {*zonghe tongxin wang*} to establish an IO communication support SoS. The joint campaign IO command institution should, based on the joint campaign IO missions, apply to the joint campaign command's {联指 *lianzhi*} communication department for the necessary channels (lines) {*xindao (xianlu)*} for the use of the IO command institution and the IO units. The various IO units via multiport facilities equipment {*duozhong jiekou shebei*} access the joint campaign integrated communication net, to ensure that the joint campaign IO command institution and all IO units [can], within the joint campaign integrated communication net, have real-time transmission of command, coordination, and intelligence information. Second is the synthetic [comprehensive] application of multiple communication means to establish IO special-direction nets {专向网 *zhuanxiang wang*}. The joint campaign IO **[end of page 212]** command institution should for its directly subordinate IO units establish special-direction nets such as for radio transceiver communication {*wuxiandian tai tongxin*}, microwave relay communication {*weibo jieli tongxin*}, and satellite communications {*weixing tongxin*}. The IO units of all services' and arms' operational groups {*zuozhan jituan*} usually rely on the joint campaign integrated communication net to effect signal communication, and when necessary they too can establish special-direction communication nets, and establish IO reconnaissance and intelligence information transmission nets. The various services' and arms' IO units should use short-wave adaptive transceivers {*duanbo zishiying diantai*}, satellite communication vehicles {*weixing tongxin che*}, tactical communication satellite terminals {*zhanshu tongxin weixing zhongduan*}, and task group mobile communication systems {*jiqun yidong tongxin xitong*} to join the joint campaign IO coordination communication net. The IO command and control [C2] system {*zhihui kongzhi xitong*} usually is established by relying on public information platforms, and when necessary it also can be established by

unified operations-research-based planning {*tongchou*} by a communications department commercially invited {商请 *shang qing*} by the IO command institution.

III. Cryptographic {*jiyao*} support…213

Joint campaign IO cryptographic support signifies cryptographic briefings {*mima tongbao*} and cryptological {*mima*} support and cryptographic equipment {*mima zhuangbei*} support activity carried out within the IO implementation process. Usually it is adjusted-coordinated and organized by the campaign cryptography department. Based on joint campaign IO needs and requirements, it relies on various communication means to establish an IO cryptographic support SoS.

Its main measures are as follows: coordination of the related departments in organizing and establishing an IO cryptographic support SoS, dispositioning {*bushu*} cryptographic support strengths, constructing a cipher telegram network {*mima dianbao wangluo*}, decoding and transmission/handling {译传办理 *yi chuan banli*} of cipher telegrams, and supporting the transmission of IO command and coordination orders in a secure {*baomi*}, rapid, and accurate manner; organizing and establishing of various types of cipher secrecy systems {*mima baomi xitong*}, to ensure the security {*anquan*} of all types of military information, weapons control {*wuqi kongzhi*}, and identification friend or foe [IFF] {*diwo shibie*} systems for IO, and that of other important operational C2 systems; and organizing and establishing of an IO cryptographic management {*mima guanli*} system, to support the use and self-security protection for all types of ciphers for IO. The basic requirement is as follows: synthetically [comprehensively] applying measures such as cryptographic technology, technology to counter EM radiation {*fang dianci fushe jishu*}, and technology to counter computer network infiltration {*fang jisuanji wangluo shentou jishu*}, so as to establish a cryptological support SoS covering the entire process and full field {*quan lingyu*} of IO, and to ensure the security and secrecy {*anquan baomi*} of IO within the transmission, use, storage, and weapons control processes. **[end of page 213]**

IV. Engineering support…214

Joint campaign IO engineering support signifies a series of activities {*huodong*} carried out by synthetic [comprehensive] application of engineering support strengths and various types of engineering support measures, to support the smooth accomplishment of IO missions. Timely and reliable engineering support measures are important means for ensuring the rapid maneuver and concealed disposition {*yinbi bushu*} of IO strengths, as well as for degrading the enemy strike effects and restricting the enemy maneuvering. The main missions of joint campaign IO engineering support are to establish an IO protective engineering SoS {*fanghu gongcheng tixi*} having comprehensive {*zonghe*} resistance capability, to construct a maneuver and counter-maneuver {*fanjidong*} engineering SoS, and to build a battlefield feedwater system.

The main measures are as follows: construction, erection, and maintenance {*weihu*} of roads and bridges within the operations area {*zuozhan diqu*}; clearing away of obstacles {*zhang'ai*}, to ensure the rapid maneuver of the IO units; organizing reconnaissance of water sources, and setup of drinking water stations and feedwater stations for machinery, vehicle, and decontamination {*xixiao*} water uses; construction of protective fortifications {*fanghu gongshi*} for the IO command institution and [IO] units, to enhance the capability for resisting enemy strikes; and exploitation of terrain and of various types of camouflage instrument equipment {*weizhuang qicai*} and engineering technical means, and adoption of artificial camouflage {*rengong weizhuang*} measures, obstruction {*zhezhang*}, camouflage painting {*micai weizhuang*}, false-target camouflage {*jiamubiao weizhuang*}, etc., for friendly {*jifang*} IO targets, to reduce the enemy's probability of detection and hit {*faxian he mingzhongde gailyu*}.

V. EM spectrum management…214

EM spectrum management signifies management and control measures {*guankong cuoshi*} adopted to strengthen the effective use of the EM spectrum by the friendly various services and arms, to reduce the influence of the EM environment on operational activities, and to support the stable, reliable, real-time, high-efficiency operation {*yunxing*} of friendly spectrum-usage {用频 *yongpin*} weapons systems. Its main missions are as follows: to plan and adjust-coordinate the use of the EM spectrum, and to adopt various countermeasures {*fangfan cuoshi*} to ensure that the IO units [can] employ the EM spectrum in a safe, stable, ordered {*youxu*}, and reliable manner.

The main measures are as follows: (1) based on the battlefield EM environment and the reality of the EM spectrum resources, as well as on the quantities and performance characteristics {*xingneng tedian*} of the IO spectrum-usage weapons and equipment, scientific planning {*guihua*} and distribution of frequencies {*fenpei pinlyu*}, to ensure the frequency-use needs {*pinlyu shiyong xuqiu*} of the various types of frequency-use weapons and equipment; (2) unified operations-research-based planning considering all factors {*tongchou jiangu*} **[end of page 214]**, including factors such as operational needs and equipment technical performance, and adoption of methods such as segmented partitioning {*fenduan huafen*}, intersecting partitioning {*jiaocha huafen*}, and organizational grouping of frequencies {*pinlyu bianzu*}, to rationally distribute and use the frequencies, so as to boost the availability {*liyonglyu*} of the spectrum; (3) ensuring, in a key point {*zhongdian*} [manner] which keeps an eye on the overall situation and grasps the critical links {*guanjie*}, the timely adjusting-coordination and processing of frequency use among all types of frequency-use consoles and stations (positions) {*tai, zhan (zhendi)*} and among the various operational activities, while avoiding self-interference and mutual interference {*zirao hurao*}, and ensuring frequency use in the main direction {*zhuyao fangxiang*}, important time segments {*shijie*}, critical positions {*guanjian buwei*}, main operational activities, and main-battle weapons and equipment; (4) implementation of full-frequency-domain {*quanpinyu*}, full-dimensional {*quanfangwei*}, full-time surveillance {*jianshi*} of the battlefield EM environment, and rigorous control {*yanmi zhangkong*} of the battlefield EM posture {*taishi*}; and

(5) timely carrying out of synthetic [comprehensive] analysis and assessment {*zonghe fenxi panduan*} of the enemy's EM spectrum use situation detected by monitoring {监测 *jiance*}, and of the situation of our implementation of EM jamming {*dianci ganrao*}, putting forth of handling recommendations {*chuzhi jianyi*} and briefing of the related departments, and guiding of the units in correct use of the frequencies, to ensure adjusted-coordinated order in frequency use and the full bringing into play of weapons and equipment effectiveness.

VI. NBC protection {*he hua sheng fanghu*}…215

NBC protection for joint campaign IO signifies the general term for various protective measures and activity adopted within the IO implementation process, when suffering an enemy nuclear, biological, or chemical [NBC] weapons raid {*he hua sheng wuqi xiji*}, or when our nuclear and/or chemical installations {*he hua sheshi*} suffer secondary harm {*cisheng weihai*} produced by an enemy raid. The use of NBC weapons will have a major influence on IO activities, and will gravely threaten the security of friendly IO personnel and of weapons and equipment. Hence, in organizing and implementing joint campaign IO, [command personnel] must attach importance to protection against NBC weapons, and strive via various protective support measures to reduce the enemy strike effects and to boost the battlefield survivability {*shengcun nengli*} of the IO personnel and equipment.

The main measures are as follows: based on the NBC threat situation, fully carrying out well the protective preparations for NBC weapons raids; concealed and decentralized deployment {*yinbi, shusan peizhi*} of the IO strengths, and at the right time effecting their maneuvering transfer {*jidong zhuanyi*}; full exploitation of favorable terrain and meteorological conditions, to strengthen engineering protection; carrying out preparations combining the use of standard {制式 *zhishi*} and simple instrument equipment; and after suffering a raid, timely ascertainment {*chaming*} of the situation, and organizing of rescue {*qiangjiu*}, rush repairs {*qiangxiu*}, and decontamination, to repair from the aftermath of the raid {*xiaochu xiji houguo*}. During activities in contaminated areas {*shouran qu*}, **[end of page 215]** [command personnel] should rigorously organize protection, to mitigate the injuries and harm to personnel.

VII. Position warning and defense…216

Position warning and defense signify security and guarding {*anquan jingwei*} measures adopted for the IO units in order to defend against the enemy's harassing attacks {*xirao*} and reconnaissance by various means. Their main goal {*mudi*} is to timely detect the signs {*zhenghou*} of the enemy's raids and enemy reconnaissance activity, so as to facilitate timely adoption of effective measures and to support the IO units in safely and smoothly fulfilling the IO missions. Within future joint campaigns, the IO units will be important targets of enemy raids, and if the IO strengths have a decentralized deployment {*peizhi fensan*}, their protection capability will be weak. Hence, strengthening of position defense and doing a good job of fortifications

construction and camouflage have particularly important significance for boosting protection [capability] and adaptability to changes {*yingbian nengli*}, and ensuring work in a concealed, safe, and stable manner.

Position warning for IO units should be grounded in self-strengths {*zishen liliang*}, thorough planning {*jihua*}, and winning over the assisting support {*zhiyuan*} of friendly neighbor units and the masses. When necessary, [command personnel] can request the higher levels to dispatch units to assist in warning. Based on the differences in the support scope, position warning and defense can be divided into ground warning {*dimian jingjie*}, surface-to-air warning {*duikong jingjie*}, surface warning {*duihai jingjie*}, mobile warning {*jidong jingjie*}, and quartering security {*suying jingjie*}.

VIII. Surveying and mapping support…216

Joint campaign IO surveying and mapping support indicates the various measures and activities adopted in surveying and mapping and navigation {*daohang*} respects, as well as battlefield environment information support respects, in order to ensure the smooth fulfillment of the IO missions. Surveying and mapping support penetrates through the entire process of IO, and is embodied within the support for all types of IO activities. Its main mission is to provide the IO command institution, C2 system, and IO equipment with integrated {*yitihua*} surveying and mapping information, geographic spatial information, navigation positioning {*daohang dingwei*}, and time and frequency standards {*shijian pinlyu jizhun*}, and surveying and mapping technical services. Future joint campaign IO will unfold {*zhankai*} before other campaign activities {*zhanyi xingdong*}, and will penetrate through the entire process of the campaign; and its corresponding surveying and mapping support similarly will unfold within the joint campaign surveying and mapping support SoS. The two will be jointly accomplished with unified planning, unified disposition, and division of labor and cooperation {*fengong xiezuo*}.

The main measures are as follows: providing battlefield basic geographic information products, with military-use maps and image maps [photomaps] {*yingxiang ditu*} as primary, **[end of page 216]** and multi-means navigation positioning services and time and frequency standards with Beidou {北斗} navigation positioning as primary, to meet the basic needs and requirements of electronic warfare [EW] {*dianzi duikang*} and network attack and defense operations {*wangluo gongfang zuozhan*}; researching the influence of natural factors (surface features, landforms, soil properties, bodies of water, vegetation {*zhibei*}, and EM) and human factors on the operational effectiveness {*zuozhan xiaoneng*} of EM equipment; preparing special-topic products, such as operations-zone {*zuozhan diyu*} road network distribution charts {*luwang fenbutu*} and information infrastructure {*xinxi jichu sheshi*} (communication stations {*tongxin taizhan*} and broadcasting stations {*guangbo diantai*}) distribution charts; and putting forth recommendations for exploiting and transforming the terrain.

IX. Meteorological and hydrological [M&H] {*qixiang shuiwen*} support…217

Joint campaign IO M&H support signifies battlefield M&H environmental support activity carried out by synthetically [comprehensively] applying various M&H support strengths, so as to smoothly implement IO command and unit activities. Its basic missions are as follows: to establish an M&H joint support SoS mutually adapted to the needs of joint campaign IO command and of unit activities; to draft {*nizhi*} M&H joint support plans; to timely provide operations area (zone) {*zuozhan quyu*} M&H background resources, and accurately prepare and distribute M&H forecasts {*yubao*} and alerts {*jingbao*}; to analyze and research the influence of adverse M&H conditions on IO activities; to put forth the corresponding countermeasures and recommendations; and to fully exploit the favorable factors to carry out IO.

The main measures are as follows: (1) under the guidance of the joint operations M&H support institution, with all operational group M&H support institutions (elements {*fendui*}) as primary and the local M&H department as supplemental {*buchong*}, building of an IO M&H joint support SoS; (2) comprehensive [synthetic] exploitation of technical means — meteorological satellites {*qixiang weixing*}, ocean satellites {*haiyang weixing*}, weather radar, M&H observation stations {*guance zhan*}, and M&H intelligence and reconnaissance {*qingbao zhencha*} — to build a comprehensive monitoring net {*zonghe jiance wang*} for the battlefield M&H environment, for timely grasp of the enemy and friendly sides' {*diwo shuangfang*} M&H situation; (3) reliance on information networks — satellite communications nets, command dedicated nets {指挥专网 *zhihui zhuan wang*}, military integrated information nets {*zonghe xinxi wang*}, and field mobile communication nets {*yezhan jidong tongxin wang*} — to build an M&H information transmission net, so as to realize interconnection and intercommunication {*hulian hutong*} of M&H support systems and information sharing {*xinxi gongxiang*}; (4) organizing of M&H forecast experts in all services and arms, establishing of M&H forecast joint consultation mechanisms {*huishang jizhi*} to jointly analyze and study the influence of battlefield M&H environments on **[end of page 217]** joint campaign IO activities, timely unified issuing of weather and hydrological forecasts and alerts to all levels of command institutions and to operational units, and putting forth of recommendations for exploiting M&H conditions favorable to us and unfavorable to the enemy, as well as measures to be adopted in view of major disastrous and dangerous weather and hydrological conditions; (5) analysis and study of the influence of M&H-space weather conditions which can occur in the IO area (zone) — strong rainfall, strong snowfall, typhoons, sea waves, eclipses, and ionospheric changes — on EM jamming activities, and timely putting forth of responsive measures and recommendations, to ensure smooth implementation of EM jamming activities; (6) mandatory decentralized deployment and disposition of important M&H support installations, and doing a good job of their concealment and camouflage; (7) strengthening of the security and defense {*anquan fangyu*} of M&H radio equipment against EM jamming, and watching the situation to organize its maneuver and evasion, or [to organize] electronic diversion/demonstration {*dianzi yangdong*} to deceive and confuse the enemy; and (8) strengthening of the warning and defense of M&H information safeguarding and

assisting support {*baozhang zhiyuan*} centers at all levels, to guard against enemy raid and sabotage {*xiji pohuai*}.

X. Battlefield management…218

Battlefield management indicates various types of management work performed by the units within the operations zone. It mainly includes the following content: position {*zhendi*} management, weapons and equipment management, and vehicle management. Its goals are to maintain battlefield order {*zhixu*}, to reduce all types of harm {*sunhai*}, and to consolidate and boost the combat power {*zhandouli*} of the units (elements). IO unit commanders at all levels must focus on the new characteristics of the modern battlefield, strengthen management and education of the units, establish a sound system for the various rules and regulations {*guizhang zhidu*}, and constantly improve management methods, to do a good job of battlefield management.

Position management signifies management of the combat living {*zhandou shenghuo*} and positional installations after the units (elements) have entered their positions. Its goal is to establish positional living order {*zhixu*} adapted to battleground needs and requirements. The positions should carry out rigorous camouflage, and strictly control the positions' egress and ingress of personnel, to guard against enemy spies sneaking in {*dite hunru*}; routinely take care to do inspections {*jiancha*}, maintenance {*weixiu*}, and hardening {加筑 *jiazhu*} of protective fortifications; based on the enemy situation {*diqing*} and the units' situation, in good time establish a day-to-day administrative management system {*zhidu*} adapted to battlefield management's information, duty watches {*zhiban*}, meeting reports [to superiors] {*huibao*}, requests for leave and reporting back after leave {请假销假 *qingjia xiaojia*}, and reports to request instructions {*qingshi baogao*}; based on the mission and season, do a good job of sanitation management {*weisheng guanli*}, to cut down on disease; and strictly protect water sources, and do a good job of food and drink sanitation {*yinshi weisheng*}, **[end of page 218]** to guard against food poisoning. In the severe cold season, they should adopt winter-proofing and anti-freezing measures {*fanghan, fangdong cuoshi*}. In the torrid season, they should guard against heatstroke; guard against intestinal-tract infectious diseases and malaria; guard against death from water-logging {水淹亡 *shuiyan wang*}; guard against poisoning from eating wild plants {*shi yesheng zhiwu zhongdu*}; and guard against mosquitoes, horseflies, leeches, and snakebites, to as much as possible avoid non-combat depletion of numbers {*feizhandou jianyuan*}.

Weapons and equipment [management] and vehicle management are important aspects in boosting the units' survival power {*shengcunli*} and in consolidating unit combat power. Their goal lies in seeing that all types of weapons and equipment remain in a good status {*zhuangtai*}, and are adapted to the needs and requirements of combat. Weapons and equipment must be routinely inspected, and properly safeguarded {*baoguan*}. Parking areas usually are chosen in points away from highways, convenient for executing missions, avoiding clear targets, having terrain concealment, convenient for constructing fortifications and for fire prevention and flood protection, and near water

sources—and given camouflage and strengthened warning, with storage of petroleum products {*youliao*} maintained at a safe distance. [Command personnel] must strengthen driving management; specify the attention items, such as driving speeds and vehicle spacing {*cheju*}, as well as camouflage, air defense {*fangkong*}, and artillery defense {防炮 *fangpao*}; [and see that drivers] abide by traffic rules {*jiaotong guize*}, submit to adjustments {*tiaozheng*} and inspections, pay attention to safety signals and signs, and execute lights and noise management specifications.

Section 2: Organization of IO Support…219

The organization of joint campaign IO support signifies the organizational and leadership activity carried out in order to accomplish IO support. Thorough organization of operational support for IO is a prerequisite and basis for smoothly implementing IO activities.

I. Establishing support institutions, collecting intelligence and data/resources {*ziliao*}…219

The joint campaign command institution is the leader {*lingdaozhe*} for IO support. It is responsible for the general planning {*zongti jihua*} and organization of IO support, directly guides the activities of its directly subordinate IO support strengths, and provides guidance for IO support to the operational groups of all services and arms. The operational group command institutions of all services and arms are the organizers and planners for the IO support internal to their root services and arms. **[end of page 219]** Their main duties are to implement all IO support-related instructions {指示 *zhishi*} from the joint campaign command institution, to organize and fulfill the IO support missions internal to the root services and arms, and, based on the higher-level unified disposition, adjusting-coordinating with the other services and arms to jointly conduct IO safeguarding and assisting support and complementary activities {*peihe xingdong*} among multiple services and arms.

Since IO activities are only one important component of joint campaign activities, in order to ensure the consistent adjusting-coordination between IO activities and a joint campaign's other operational activities, and to concentrate {*jizhong*} support strengths, under ordinary circumstances IO does not by itself organize and build an independent IO support department. Instead, it brings the operational support missions of IO into the midst of the general missions of joint campaign operational support, carries out unified operations-research-based planning {*tongyi chouhua*}, and unifies its implementation. Usually the IO departments within the joint campaign command institution and within the operational group command institutions of the services and arms will be responsible for providing the operational support needs to the various operational support teams {*xiaozu*} or operational support centers; and the various operational support teams or operational support centers do the specific operations-research-based planning and implementing of the support activities for joint campaign IO, including communication, engineering, chemical defense {*fanghua*}, meteorology, hydrology, and surveying and mapping.

Between the various operational support teams or operational support centers and the IO departments there is a coordination and complementation relationship {*xietong peihe guanxi*}.

Full and reliable IO support intelligence and data/resources are the basic foundations for implementing IO support decision-making {*juece*} and for organizing IO support activities. Their sources mainly include channels in three respects: the higher level's IO support instructions, plans, and notices {*tongzhi*}; the information acquired by the root level directly via reconnaissance means; and briefings by friendly neighbor units and local departments. Their content mainly should include the following: the basic requirements of the root-level senior officer {*benji shouzhang*} and the higher-level command institution for IO support; the basic situation of the personnel and equipment of the IO strengths and support strengths; the assisting support {*zhiyuan*} which can be provided by the higher levels, friendly neighbors, and local support-the-front institutions {*difang zhiqian jigou*}, and the scale and time opportunities {时机 *shiji*} of the attached {*peishu*} IO support strengths; the situation of the enemy force-strength task organization {*bingli biancheng*} and disposition, as well as of weapons and equipment and personnel; and the operational support-correlated natural and socio-humanistic {*shehui renwen*} situation within the operations area, including its terrain, hydrology, meteorology, traffic, and population. **[end of page 220]**

II. Putting forth support reports and recommendations…221

In the campaign preparations phase, the operational support department should join with the IO department to perform analysis and assessment on the basis of an all-around grasp of the correlated intelligence and information, and then promptly put forth to the commander their reports and recommendations related to the support aspects of IO. Their content mainly includes the following: the enemy's operational intention {*zuozhan qitu*}; the reconnaissance, jamming, and strike means which can be adopted for our IO strengths and support strengths; the battlefield environment's possible influence on IO support; the basic missions and objects {*duixiang*} of support for friendly IO support; the IO support measures and the basic disposition of IO support strengths, as well as the support coordination methods.

III. Drafting the support plan {*jihua*} and instructions…221

After determination of the IO support resolution, it is generally issued in the form {形式 *xingshi*} of instructions accompanying the IO orders, or is issued by directly bringing it into the units' general support instructions. It serves as the basic foundation for operations-research-based planning of IO support. The IO support plan is the specific arrangements or general plan {*zongti guihua*} for organizing and implementing IO support, and is an important component of the IO plan. Usually it is drafted based on the IO support instructions. The IO support plan according to its content and use is differentiated into an IO support comprehensive plan {*zonghe jihua*} and special-project plan {专项计划 *zhuanxiang jihua*}. The comprehensive plan is a general-quality plan

{*zongtixing jihua*} relating to the IO support activities, while the special-project plan is a plan for a certain specific {*teding*} operational support activity.

IV. Supervising-guiding {督导 *dudao*} the implementation of support preparations…221

Whether the IO support preparations work is sufficient has a direct influence on the smooth fulfillment of the IO support missions. In order to ensure that the IO support personnel, equipment, materiel {*wuzi*}, and instrument equipment {*qicai*} are in a good status, [to ensure] the high-quality implementation of all support preparations measures, and to seize the initiative {*zhudongquan*} in IO support, the operational support institutions and operational institutions at all levels must strengthen the supervising-guiding and inspections of the IO support preparations work, at all times grasp the situation of the progress of the support preparations work, and promptly detect [any] problems and correct them. **[end of page 221]** The key point {*zhongdian*} content of inspections of the IO support preparations work mainly includes the organizational grouping and mobilization {*dongyuan*} of IO support strengths; the plan for support activities; the requests for, allocation {*diaopei*} of, and transportation {*shusong*} of weapons and equipment, materiel, and instrument equipment; the collection of support intelligence information; the organization of coordinated actions {*xietong dongzuo*} among the support strengths; and the launch {*kaizhan*} of the support institutions' pre-combat training {*zhanqian xunlian*}.

V. Grasping the situation and controlling the support activities…222

In order to ensure the smooth realization of the IO support's predetermined objectives {*yuding mubiao*}, during the operational process, the operational support institutions at all levels must timely grasp the support situation of battlefield IO, and timely adopt adjustment and control {*tiaokong*} measures. The situations which require key point understanding and grasp mainly include the following: the situation of the progress of the IO support missions; whether the disposition and activities of the support strengths mutually conform to the actual situation of the battlefield; and the attrition/depletion {*xiaohao*} situation of the support personnel, equipment, materiel, and instrument equipment. The control of the IO support activities mainly is differentiated into two types: planned control {*jihua kongzhi*} and ad hoc control {*suiji kongzhi*}. Planned control mainly is employed under circumstances where the discrepancies {*churu*} between the battlefield situation and the pre-combat estimated {*yuji*} situation are not large. Ad hoc control mainly is applicable to temporarily arising outbreak situations {*tufa qingkuang*} within IO support, or is used when the changes between the battlefield situation and the anticipated {*yuxiang*} situation are fairly large. Control of IO support activities usually includes four links {*huanjie*}: issuing the support instructions {*xiada baozhang zhishi*}, monitoring {监控 *jiankong*} the battlefield posture {*zhanchang taishi*}, evaluating-appraising {*pinggu*} the support effects, and correcting activities deviations {*jiuzheng xingdong piancha*}. The associated control instructions {*zhiling*} generally are issued in the form of supplemental support instructions {*buchong baozhang*

zhishi}. When necessary, [command personnel] also can directly carry out on-the-spot supervising-guiding {*xiandi dudao*} of these activities via the mode of dispatching inspection teams {*jiancha zu*} to the IO support units (elements).

Section 3: Requirements for IO Support…222

A good many characteristics possessed by operational support for joint campaign IO, the subordinate quality {*congshuxing*} of the support position {*diwei*}, the arduousness of the support missions, the multidimensionality {*duoyuanxing*} of the objects of support, **[end of page 222]** and the extensiveness {*guangyanxing*} of the activities space {*xingdong kongjian*}, have determined that in terms of organization and implementation, joint campaign IO support must meet the following several requirements.

I. Complying with the senior officer's intent {*shouzhang yitu*}…223

The fundamental mission of IO support is to ensure the realization of the operational resolution {*zuozhan juexin*} of the IO commander. Whether operational support can be mutually adapted to the IO missions and disposition, and embody the intent and requirements of the IO commander, are important standards {*biaozhun*} for judging the quality of operational support. In terms of mutual relationships, IO activities occupy the leading position, while IO support activities occupy the subordinate position. Hence, IO support must, on the basis of an all-around understanding of the intent and requirements of the IO commander, center on the general disposition of IO activities, to scientifically and rationally carry out IO support decision-making; formulate IO support plans; adjust-coordinate and control the IO support activities; and ensure that the essential factors {*yaosu*} — the objects of support, organizational grouping of support, support methods, and support time — are mutually adjust-coordinated consistently with the IO activities, to enhance the directed [focused] quality {*zhenduixing*} of operational support.

II. Laying stress on the support key points…223

The joint campaign IO strength composition {*liliang goucheng*} is complex, the activities modes {*xingdong fangshi*} are diverse, and the IO support missions are extremely strenuous. The contradictions {*maodun*} between IO support capability and its support needs are comparatively prominent. In order to ensure the fulfillment of the IO support missions and to boost the support benefit, [command personnel] must focus on the full process of entire IO; scientifically determine the support key points; concentrate the main support strengths, and insert them into the critical operational directions {*guanjian zuozhan fangxiang*}, critical operational activities, and critical operational time segments {*guanjian zuozhan shijie*} having the most influence on entire IO, to form and maintain relative superiority {*xiangdui youshi*} in support strengths, try their best to avoid seeking perfection by decentralizing {以散求全 *yisan qiuquan*}, keep their options open {坚持有取有舍 *jianchi youqu youshe*}, distinguish between the primary and the

secondary {主次分明 *zhuci fenming*}, and implement support in a manner having key points.

III. Emphasizing joint support…223

Joint campaign IO is the synthetic [comprehensive] application of integrated-whole-quality {*zhengtixing*} information offense and information defense by multiple means, including EW {*dianzizhan*}, network warfare {*wangluozhan*}, psychological warfare [PSYWAR] {*xinlizhan*}, operational secrecy {*zuozhan baomi*}, military deception {*junshi qipian*}, and entity destruction {*shiti cuihui*}. **[end of page 223]** The requirements on the application of the various types of IO strengths for IO support are mutually different. For example, the EW strengths and entity destruction strengths usually have fairly stringent requirements for meteorological, hydrological, and surveying and mapping support. The requirements of the network warfare and PSYWAR strengths for geographic environmental information support are relatively low, but their requirements for socio-humanistic information support then are fairly stringent. Thus, IO support must keep in mind the integrated-whole quality of IO activities; focus on the characteristics of the various types of IO strengths; and synthetically apply the professional {*zhuanye*} and nonprofessional operational support strengths of all services and arms, as well as the local support-the-front strengths, to implement joint-quality support {*lianhexing baozhang*} under unified command {*tongyi zhihui*}, and integration {*yitihua*} of support strengths and support means, to ensure the smooth fulfillment of the various operational support missions of IO.

IV. Maintaining continuous stability…224

The joint campaign IO scale is large, its intensity high, its duration {*chixu shijian*} relatively long, and its operational support strength attrition {*xiaohao*} fairly high. In order to ensure seizing and maintaining information dominance within the entire campaign implementation process, [command personnel] must emphasize the continuity {*lianxuxing*} and stability of IO support, and implement uninterrupted support. They must keep in mind the entire process of joint operations; fully foresee {*yujian*} the situations which can arise in each operational phase; formulate multiple adaptive courses of action [COAs] {*yingbian fang'an*}; rationally differentiate the employment of the support strengths; leave certain numbers of reserve {*yubei*} support strengths and mobile support {*jidong baozhang*} strengths; and do well in the supplemental allocation {*buchong diaopei*} of support personnel, equipment, and instrument equipment within the operational process—so as to enhance the elasticity {*tanxing*} of the operational support disposition and to support the continuous stability of the support activities. **[end of page 224; end of chapter]**

Chapter 12
Joint Campaign Information Operations Logistics Support…225

Joint campaign information operations (IO) logistics support {*houqin baozhang*} indicates the general term for the various support measures implemented, and corresponding activity {*huodong*} carried out within joint campaigns, in order to meet the needs and requirements {*xuyao*} of the IO units {*budui*} in operational and daily-life respects, by various logistics-related professional departments {*zhuanye bumen*} and units (elements) {*bu (fen) dui*}, in materiel {*wuzi*}, technology, medical treatment, and transport {*yunshu*} respects.[10] Its basic missions are as follows: to use the logistics strengths {*liliang*} within the task organization {*biancheng*} and the local support-the-front strengths {*difang zhiqian liliang*} so as to provide the IO units with support for funding {*jingfei*}, materiel, logistics, and transport; to consolidate and boost the operational capability {*zuozhan nengli*} of the IO units; and to support the IO units in smoothly fulfilling their operational missions {*zuozhan renwu*}.

Section 1: Logistics Support Requirements…225

Within joint campaigns, to center on the fulfillment of the IO units' missions, the organization and implementation of logistics support should satisfy the following requirements.

I. All-around preparations, boosting quality…225

In joint campaigns under informationized conditions {*xinxihua tiaojianxia*}, the surprise quality {*turanxing*} is increased and the operational tempo {*zuozhan jiezou*} is unusually rapid. This requires that IO logistics support must do a good job of the various types of preparations work, and, while ensuring its time effectiveness quality {*shixiaoxing*}, as much as possible boost the support quality. Its preparations work not only must **[end of page 225]** be carried out in peacetime, but also must be carried out before imminent battles {*linzhan qian*} and within operations. First is the need to do a good job of the peacetime preparations work. [The logistics department] should, based on the joint campaign IO mission needs and requirements, draft {*nizhi*} and perfect various logistics support courses of action [COAs] {*fang'an*}, and, in a manner having a directed [focused] quality {*zhenduixing*}, perform some work which is difficult to complete during the imminent battle preparations {*linzhan zhunbei*}. For example, it can center on IO exercises {*yanxi*} and training activity {*xunlian huodong*} to organize and implement some logistics drills {*yanlian*}, so as to become familiar with the battlefield environment,

[10] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

the support missions, and the support COAs. Second is the need to do a good job of the imminent battle preparations work. After receiving the in-advance orders {*yuxian haoling*}, it should swiftly carry out imminent battle mobilization {*linzhan dongyuan*} and training of the logistics strengths, establish and improve the logistics command and support institutions, revise {*xiuding*} the logistics support COAs, adjust and replenish the materiel reserve {*tiaozheng he buchong wuzi chubei*}, perfect the rear engineering installations {*houfang gongcheng sheshi*}, and at the right time unfold {*zhankai*} the logistics strengths. Third is the need to do a good job of preparations work during combat. After launch of the campaign, the logistics department must be grounded in the most difficult, most complex situations to carry out forecasting {*yuce*}; take the initiative {*zhudong*} to understand the situations which can arise within each phase and within the various operational activities {*zuozhan xingdong*} of the campaign; ahead of time, do a good job of all items of preparations work; and formulate multiple adaptive measures {*yingbian cuoshi*}, to ensure providing continuous, timely, and reliable logistics support for the IO units during the operational process.

II. Unified operations-research-based planning considering all factors {*tongchou jiangu*}, key point {*zhongdian*} support…226

Within joint campaigns, since the IO activities scope is broad and the missions strenuous, the result is that the contradiction {*maodun*} between the integrated-whole {*zhengti*} logistics support capability for IO and the support needs {*xuqiu*} is unusually prominent. In order to ensure that the IO units fulfill the IO missions entrusted by the higher levels, the logistics support organs {*jiguan*} must in a rational, centralized {*jizhong*}, and flexible {*linghuo*} manner employ the logistics support strengths to carry out key point support.

First of all, they should do unified operations-research-based planning considering all factors, and lay stress on the objects {*duixiang*} of key point support. First is key point support for the units (elements) executing strategic and campaign {*zhanlue, zhanyi*} IO missions. Second is key point support for the units (elements) executing IO missions on the main battlefield, in the main operational direction {*zhuyao zuozhan fangxiang*}, and in important operations areas {*zuozhan diqu*}. Third is key point safeguarding and assisting support {*baozhang zhiyuan*} for units undertaking {*danfu*} the main operational mission(s).

Next, they should pay close attention to the critical operational time segments {*guanjian zuozhan shijie*}, and lay stress on the key point support time opportunities {时机 *shiji*}. **[end of page 226]** The core mission of joint campaign IO is to assist-support and complement {*peihe*} the operational activities of the other operational strengths {*zuozhan liliang*}. Hence, the critical time segments for the joint campaign IO units to execute their IO missions are precisely the critical time opportunities for logistics support. The IO unit logistics commander {*houqin zhihuiyuan*} should at all times understand the development situation of campaign operations, carry out conscientious analysis and assessment {*panduan*}, accurately {*zhunque*} grasp the critical time

segments of campaign operational activities, and concentrate strengths {*jizhong liliang*} to implement support having key points.

Third, they should [conduct] all-around analysis, laying stress on the key point support links {*huanjie*}. Commanders, while paying close attention to the objects of key point support and to the support time opportunities, also must in an all-around and uninterrupted {*bujianduan*} manner analyze the fulfillment situation of the logistics support missions. This includes the changing situation and distribution situation of the logistics support strengths, as well as the main contradictions and secondary contradictions within the supply and demand relationship {*gongxu guanxi*}. Within these, they [must] concentrate on the support links which require key point attention, and from start to finish place these key point support links in the most important position of the logistics support missions.

III. Close coordination {*miqie xietong*}, bringing into play composite strength {*heli*}…227

Joint campaign IO logistics support missions are strenuous, [so] relying on a single support strength or on the support strengths within the organizational system {*jianzhi*} would make it difficult to meet the actual needs and requirements of operations. The commander must properly organize the coordination of all types of support strengths and bring into play their composite strength, to ensure the fulfillment of the logistics support missions. He must establish a unified command institution {*tongyide zhihui jigou*}; fully exploit the IO units' original logistics strengths; absorb the logistics strengths of the reinforcing and attached units {*jiaqiang he peishu budui*}, as well as the support strengths of the local assisting support {*difang zhiyuan*}; closely adjust-coordinate {*miqie xietiao*} the activities of the various types of support strengths; unify the allocation and use {*tongyi diaopei shiyong*} of materiel and instrument equipment {*wuzi qicai*}; and unify the organization of battleground transport {*zhandi yunshu*} and logistics defense {*houqin fangwei*}. He must strengthen the awareness of integrated-whole cooperation {*zhengti xiezuo*}, establish the thought of the local situation being subordinate to the overall situation {*jubu fucong quanju*}, unify the adjustment and control {*tongyi tiaokong*} of the support activities in all directions and all time segments, see that the operations {*yunzhuan*} of the various support strengths center on the unified intent {*tongyide yitu*}, and to the maximum extent bring into play the integrated-whole effectiveness {*zhengti xiaoneng*} of logistics support.

IV. Rapid reaction, active complementation {*jiji peihe*}…227

The surprise quality and rapid tempo of joint campaign operational activities require that logistics be able **[end of page 227]** within the shortest time to concentrate sufficient strengths, and with the most rapid reaction speed actively provide the IO units with powerful support, to ensure the implementation of all activities of the IO units and the fulfillment of all missions. First is the need to strengthen the foresight quality {*yujianxing*} of logistics support, all-around analyze the various situations which can

occur on the battlefield, focus on the different situations to anticipate {*yuxiang*} the various support COAs, and center on the support COAs to carry out solid and careful preparations. Second is the need to bring into play the active quality {*jijixing*} of support work, take initiative to understand and grasp the needs of the IO units for logistics support, and fully complete the forward delivery {*qiansong*} of materiel and the rear transport {*houyun*} of the wounded. Third is the need to boost the time effectiveness quality of the support work, simplify the work procedures {*chengxu*}, and fully put to use advanced command information systems {*zhihui xinxi xitong*}, to accelerate the transmission {*chuandi*} and feedback of various types of support information. Fourth is the need to as much as possible reduce the support links, forward deploy {*kaoqian peizhi*} the support institutions, and synthetically [comprehensively] apply {*zonghe yunyong*} various support means to organize rapid and uninterrupted support.

V. Strengthening of defense {*fangwei*}, boosting survivability {*shengcun nengli*}…228

Within joint campaigns, the logistics command institutions, support personnel, materiel and equipment, and traffic and transport lines [lines of communication and transport] {*jiaotong yunshu xian*} will be subject to the enemy's strikes with multidirectional, multilevel {*duocengci*}, integrated firepower {*zonghe huoli*}; and the safety of logistics will directly impact the fulfillment of the logistics support missions, and impact the fulfillment of the IO units' basic missions. Hence, [commanders] must strengthen the security and defense {*anquan fangwei*} of logistics support data {*zhuyuan*}, to boost its survivability. First is the need to bring logistics security and defense into the midst of the integrated-whole defense plan {*zhengti fangwei jihua*} for the IO units, and to place it in a position of equal importance to the IO units, for providing the protection. Second is the need to carry out this protection, with logistics deployment zones {*peizhi diyu*} and lines of communication {*jiaotongxian*} as the key points. Third is the need to uphold the principle of "a combination of defense and strike {*fangda jiehe*}, with defense as primary," and to synthetically adopt multiple "concealment" and "deception" {"藏," "骗" *"cang," "pian"*} means to carry out the protection. Fourth is [adopting] a mutual combination of defense of single logistics targets {*houqin mubiao*} and defense of support areas {*baozhangqu*}, and a mutual combination of self-defense {*zishende fangwei*} of the logistics support strengths and screening {*yanhu*} by operational units. **[end of page 228]**

Section 2: Organizational Grouping and Disposition {*bianzu yu bushu*} of Logistics Support Strengths…229

I. Organizational grouping of logistics support strengths…229

The organizational grouping of joint campaign IO logistics support strengths signifies the scientific combination carried out over the IO logistics support strengths, in order to make it easy to carry out the support missions. Usually it is specifically {*juti*} organized and implemented by the IO logistics support department, according to the IO

commander's general intent {*zongti yitu*}, and based on the situation of the classes {*zhonglei*} and numbers of support missions and support strengths.

The joint campaign IO logistics support strengths usually have a task organization [composed] of the logistics support strengths within the root-level organizational system {*benji jianzhi*}, the higher-level [dispatched] reinforcing logistics support strengths, the local accompanying support-the-front {地方随军支前 *difang suijun zhiqian*} logistics support strengths, and the logistics support strengths of the attached units (elements). With respect to the above various types of support strengths, [the IO logistics support department personnel] should uphold the principle of "as much as possible preserving the organizational system, ensuring jobs suited to professional training {*zhuanye duikou*}, and conscientiously boosting the benefit," to carry out unified operations-research-based planning {*tongyi chouhua*} and organizational grouping. The organically assigned strengths {*jianzhi liliang*} of the IO units' root-level logistics are the backbone strengths for carrying out the IO logistics support missions, and during their organizational grouping their original organizational system should as much as possible be preserved. The higher-level [dispatched] reinforcing logistics support strengths in principle are, per their profession, organizationally grouped into the organically assigned strengths of the IO units' root-level logistics; but when the strengths are fairly large, they also can be separately organizationally grouped for employment. The local support-the-front logistics support strengths can, based on needs and requirements, respectively be woven into the related logistics elements, and generally do not have a separate organizational grouping for carrying out missions. The higher-level logistics reinforcing strengths for attached IO units usually directly provide logistics support for the attached IO units, but also can be organizationally grouped for unified use together with [those units'] logistics organically assigned strengths.

II. Disposition of logistics support strengths…229

The joint campaign IO logistics support strengths usually are, based on the professional nature of the different strengths, respectively task organized {*biancheng*} into the corresponding command essential factors {*yaosu*} and support essential factors. When the disposition of the IO units takes the form {形式 *xingshi*} of groupings {*qun*}, the logistics support strengths can be given a unified task organization into comprehensive {*zonghe*} **[end of page 229]** support groupings, with internal setups {内设 *neishe*} of command posts {*zhihui suo*}, medical aid stations [first-aid posts] {*jiuhu suo*}, fuel depots {*youliaoku*}, quartermaster depots {*junxuku*}, and transport elements {*yunshu fendui*}. When the IO units form an echelon disposition {*tici bushu*}, usually some medical strengths {*weiqin liliang*} are taken as primary, and the units are allocated the corresponding materiel and transport power {*yunli*}, and task organized into a forward-echelon {*qiantidui*} support grouping, while the remaining logistics strengths are task organized into a rear-echelon {*houtidui*} support grouping. When the IO units have a per-direction disposition {*anfangxiang bushu*}, usually the greater part of the logistics support strengths are task organized into a main-direction support grouping, while some logistics support strengths are task organized into a secondary-direction support

grouping. When the IO units have a per-direction echeloned disposition {*anfangxiang chengtici bushu*}, the elite {*jingrui*} logistics support strengths are task organized into a forward-echelon main direction support grouping, some strengths are task organized into a forward-echelon secondary direction support grouping, and the remaining strengths are task organized into a basic support grouping. When the IO units adopt an echeloned, per-direction, or per-direction echeloned dispositional form, and the logistics support strengths are task organized into two or more support groupings, the internal organizational grouping of the rear-echelon and main-direction or basic support groupings is basically the same as the internal organizational grouping of the support groupings when they form a group disposition {*jituan bushu*}. The internal organizational grouping of the forward-echelon (secondary-direction) support grouping can be determined based on the IO support mission and the actual situation of the strength scale, and generally has an internal setup of a command team {*zhihui zu*}, medical aid station, integrated depot {*zongheku*}, and transport element. While organizationally grouping the root-level logistics support institutions, [the IO logistics support department] also should, based on the lower-level logistics support missions and the support capability situation, as well as the current state {*xianzhuang*} of the root-level logistics strengths, appropriately transfer {*choudiao*} some strengths to carry out treatment and evacuation {*jiuzhi, housong*} of the wounded, and provide the necessary reinforcement {*jiaqiang*} for the IO units (elements) undertaking the main IO mission and executing independent IO missions, to enhance their logistics support capability.

Section 3: Logistics Professional Services {*zhuanye qinwu*} Support and Preparations…230

I. Logistics professional services support…230

Within joint campaigns, the IO professional services logistics support mainly includes **[end of page 230]** materiel support, medical {*weiqin*} support, traffic and transport support, and funding support.

(1) Materiel support

Materiel support for the joint campaign IO units is the general term for the activity of raising {*chouji*}, reserve {*chubei*}, replenishment {*buchong*}, management, and supply {*gongying*} of military materiel needed for the IO units. It is an important component of joint campaign logistics materiel {*houqin wuzi*} support, and is the material {*wuzhi*} foundation which the IO units rely on for survival and operations. Its main missions are as follows: to organize the acquisition {*choucuo*}, reserve, replenishment {*buji*}, and management of the operational and daily-use materiel needed by the IO units, such as petroleum products {*youliao*}, provisions, bedding and clothing {被装 *beizhuang*}, medicinal materials {*yaocai*}, field barrack utensils {*yezhan yingju*}, and construction-project {*jijian gongcheng*} building materials. The logistics support department should, based on factors {*yinsu*} such as the campaign pattern {*zhanyi yangshi*}, the IO mission, the campaign duration {*chixu shijian*}, and the number of

participating personnel, as well as the possible casualties, storage and transport {*chuyun*} conditions, and the possible materiel attrition {*wuzi sunhao*}, make estimates {*yuji*} of the material needed by the IO units, thoroughly formulate materiel support plans {*jihua*}, and adopt multiple modes {*fangshi*} and means to continuously and effectively perform the support work for all types of materiel.

Fuel {*youliao*} support: This mainly indicates the reserve and replenishment of petroleum products. The units' petroleum products reserve is composed of three components: the carried load {*xiexingliang*}, the operating load {*yunxingliang*}, and the amplified load {加大量 *jiadaliang*}. The carried load indicates the quantities of petroleum products carried in the fuel tanks of equipment such as the equipment platforms and construction power machinery within the units' task organization. The operating load is the quantity of petroleum products carried per specifications in all levels of logistics depots of the units and by the professional elements. The amplified load is, based on the units' operational needs and requirements, the quantity increased beyond the carried and operating loads {*xieyunxing liang*}. The size of the units' fuel reserve should be rationally determined based on the missions undertaken by the IO units and the degree of difficulty of replenishment during operations, and within the reserve standards specified by higher levels. Under the usual circumstances, the IO units which independently execute missions should have an appropriately greater reserve of some petroleum products.

Quartermaster materials {*junxu wuzi*}: Based on the battlefield's actual situation, quartermaster materials support for the IO units can flexibly adopt the modes of rear supply {*houfang gongji*} and on-the-spot supply {*jiudi gongji*}. Rear supply is the mode in which the IO units rely on the higher-level logistics support strengths to carry out quartermaster **[end of page 231]** materials acquisition. The varieties of rear supply usually include standard field rations, food and drink equipment and instrument equipment, and bedding and clothing packs {*beifu zhuangju*}; and under special {*teshu*} conditions, they also include uncooked fresh (convenience) foods and daily-use articles. On-the-spot supply is the mode in which the IO units exploit local materials within the operations area to carry out acquisition. Its main varieties include uncooked fresh (convenience) foods and daily-use articles. The replenishment of quartermaster materials should, with higher-level forward delivery replenishment as primary, be carried out by adopting level-by-level and bypassing {*zhuji, yueji*} methods, as well as accompanied and air-drop (air-transport) {*bansui, kongtou (yun)*} methods. Under circumstances where the higher-level transport power is strained, replenishment can be obtained from the root level. When higher-level supply is interrupted, and the individual IO units also urgently need materials, the method of regulated replenishment {调剂补给 *tiaoji buji*} can be adopted, to resolve the urgent needs of the related IO units. When the enemy situation threat {*diqing weixie*} on the replenishment route is fairly high, [the logistics support department] should organize force-strengths and firepower escorts (convoys) {*husong*}, and put into effect forced replenishment {*qiangxing buji*}.

Medicinal materials support: Wartime medicinal materials include battlefield first-aid medicines {战救药材 *zhanjiu yaocai*} and wartime standing medicines {*changbei yaocai*}. Battlefield first-aid medicines are medicinal materials specially provided for the use of battlefield treatment of the wounded {战伤救治 *zhanshang jiuzhi*}. Generally the needed and required quantities {*xuyaoliang*} of medicinal materials are calculated by the medical departments at all levels, according to the estimated total numbers of wounded. When the needed and required quantities exceed the carried and operating loads, then the size of the excess is the amplified size; when the needed and required quantities do not exceed the carried and operating loads, then the reserve [is calculated] per the carried and operating loads. The supply methods for battlefield first-aid medicines, usually based on needs and requirements, are a mutual combination of unit supply {基数供应 *jishu gongying*} (as primary) and single-variety supply, and a mutual combination of forward delivery replenishment {*qiansong buchong*} (as primary) and self-obtained replenishment {自领补充 *ziling buchong*}. Wartime standing medicines are the consumptive {*xiaohaoxing*} medicinal materials needed and required for wartime support for outpatient {*menzhen*} and inpatient treatment {留治 *liuzhi*} of the sick and wounded. The varieties and quantities of these medicinal materials in the reserves of medical treatment institutions at all levels should be determined based on the treatment scope, number of beds, and the number of personnel in the units' organizational structure {*bianzhi*}.

Camp materiel and instrument equipment {*yeying wuzi qicai*} support: Camp materiel and instrument equipment is divided into bivouac equipment and instrument equipment {*suying zhuangbei qicai*}, lighting equipment and instrument equipment, dimming {取暖 *qu'ai*} equipment and instrument equipment, water-storage and water-transport equipment and instrument equipment, and barrack utensils.

(2) Medical support

Medical support for the joint campaign IO units is **[end of page 232]** the general term for the measures and activity of applying medical means to restore the effective strength {*yousheng liliang*} of the IO units, and of the various types of medical treatment and epidemic prevention {*weisheng jiuzhi, fangyi*} work to preserve the operational capability of the IO units. Within future joint campaigns, the enemy and friendly sides' confrontations {*diwo shuangfang duikang*} will be sharp, and the wide-ranging application of various types of high-tech weaponry {*bingqi*} on the battlefield, particularly following on the clear boosts in the position and role {*diwei zuoyong*} of IO, will cause clear increases in the IO units' casualty rates {*shangwanglyu*}, and make the medical support missions unusually arduous. The main such missions are as follows: to carry out rescue {*jiuhu*}, medical treatment, and evacuation of the IO units' sick and wounded, and to organize the IO units in carrying out sanitation work and epidemic prevention and protection {*weisheng fangyi yu fanghu*}, so as to the maximum extent restore and preserve the combat power {*zhandouli*} of the IO units. The logistics support department should, based on factors such as the campaign pattern, the IO missions, the campaign duration, the kill characteristics {*shashang xingneng*} of enemy weapons, and

the units' protection capability {*fanghu nengli*}, as well as the battlefield environment, make estimates of the IO units' medical-related depletion of numbers {*weisheng jianyuan*}; thoroughly formulate medical support plans; and adopt multiple channels, modes, and means to actively do a good job in the work of treatment and evacuation of the sick and wounded, and of sanitation work and epidemic prevention and protection. Medical support work mainly includes the content of classification of depletion of numbers {*jianyuan fenlei*}, estimation of the operational depletion of numbers, and treatment and evacuation of the wounded, as well as sanitation work and epidemic prevention and protection.

Classification of depletion of numbers: This means the differentiation carried out for the related personnel who have been withdrawn from combat {*tuichu zhandou*} due to loss of operational capability.

Estimates of operational depletion of numbers: For the convenience of the logistics department in formulating medical support plans, the rational differentiation and use of medical strengths should be estimated based on factors such as the strike activities which the enemy during operations can conduct against our IO strengths, the IO units' protective measures and deployment density {*peizhi midu*}, the operational duration, and the reference rates of depletion of numbers {*jianyuanlyu*} from past operations.

Treatment and evacuation of the wounded: The medical strengths should timely carry out treatment and evacuation of the sick and wounded. The organizational form of wartime treatment of the sick and wounded should be determined based on the battlefield environment, the allocation {*peibei*} of personnel to all levels of rescue organizations {*qiangjiu zuzhi*}, the technical levels {*shuiping*}, and the facilities equipment {*shebei*} conditions. Within joint campaigns, due to the wide front {*zhengmian*} and great depth {*zongshen*} of operations by the IO units, [the logistics department] usually adopts **[end of page 233]** the method of level-by-level treatment {*fenji jiuzhi*}. That is, all levels of treatment institutions have a deep-echelon deployment {*zongshen tici peizhi*} along a certain evacuation direction, are linked up with one another {*huxiang xianjie*}, and respectively fulfill their individually undertaken medical treatment and evacuation missions.

Sanitation work and epidemic prevention and protection: The joint campaign battlefield environment is complex, the operational tempo is rapid, the survival conditions are harsh, and there is the possibility of meeting with threats from enemy nuclear, biological, and chemical [NBC] weapons {*he, sheng, hua wuqi*}. The officers and men (of the PLA) {*zhizhanyuan*} for long periods will be in the midst of exhaustion, and will very easily catch and transmit {*chuanran*} various types of disease. The medical department should place the key points on inspecting {*jiancha*} the operations area's infectious disease and water supply situation; on supervising-promoting {*ducu*} the units in strengthening position sanitation management {*zhendi weisheng guanli*}, implementing various sanitation systems {*weisheng zhidu*}, and doing well in sanitation for field fortifications {*yezhan gongshi*} and underground tunnels; and on exploiting

favorable time opportunities, such as unit rest and reorganization {休整 *xiuzheng*} and operational intervals {*zuozhan jianxi*}, to organize sanitation personnel in going deep into the positions to conduct disease surveys, and to guide and launch anti-epidemic work and treatment of the sick and wounded.

(3) Traffic and transport support

Traffic and transport support for the joint campaign IO units is the personnel, equipment, and materiel transportation activity {*shusong huodong*} conducted so that the IO units fulfill their operational missions. Within future joint campaigns, the enemy certainly will adopt various means to carry out blockade and sabotage {*pohuai*} of our transport lines {*yunshuxian*}, which will bring about unusually great difficulty for the transport work and make the traffic and transport support missions unusually arduous. The main missions of this support are as follows: to organize and employ the campaign transport strengths and IO unit transport strengths, as well as the local support-the-front transport strengths, in implementing unit mobile transport {*budui jidong yunshu*} and materiel supply transport, and evacuation of the sick and wounded and of damaged equipment {*sunhuai zhuangbei*}, to support the IO units in smoothly fulfilling the operational missions. The logistics support department should, based on factors such as the operational pattern, the IO missions, the campaign duration, the participating personnel, the quantities and distribution of equipment, the reserve and replenishment load {*bujiliang*} of materiel, the evacuation load {*housongliang*} of sick and wounded and of combat-loss equipment {*zhansun zhuangbei*}, the terrain, the roads (air routes) {*dao (hang) lu*}, and the transport distances, make in-advance plans {*yuxian jihua*} for the IO unit transport support missions, thoroughly formulate traffic and transport support plans, and adopt multiple avenues and modes to organize and perform the traffic and transport support work for the IO units. Traffic and transport support work mainly includes the organization and use of transport power **[end of page 234]** and the determination of the transport modes and methods, as well as the organization of transport safety and defense {*anquan fangwei*}.

Organization and use of transport power: The logistics support department must meticulously organize and employ various transport strengths to bring into play to the maximum extent the effectiveness of the various means of transport {*yunshu gongju*}, and fulfill the support missions. First is the need for centralized, unified employment {*jizhong tongyi shiyong*} of transport power. [This means] implementing unified planning {*tongyi jihua*} and unified scheduling and use {*tongyi diaodu shiyong*} of the various logistics strengths, the latent {*qianzai*} logistics strengths, and the various types of transport power within the operational task organization {*zuozhan biancheng*}, and giving preference {*youxian*} to supporting the units executing the main IO mission(s) and to the transport of the main materiel. Second is the need to fully bring into play the effectiveness of the various types of transport power. Based on the battlefield geographic conditions and on the strong points of the various types of transport power, [this involves] rationally using transport power in a way adapted to local conditions {因地制宜 *yindi zhiyi*}; capably carrying out the linkup of the various links, including loading,

transport, and unloading {*zhuang, yun, xie*}; and fully exploiting the return-trip transport power {*huicheng yunli*}, so as to tightly combine {*jinmi jiehe*} forward transport {*qianyun*} and rear transport. Third is the need to preserve the sustained operating capability {*chixu gongzuo nengli*} of transport power, so that the vehicles remain in a good technical status [configuration] {*jishu zhuangtai*}. Fourth is the need to control a certain quantity of reserve transport power, so as to deal with the needs and requirements of urgent {*jinji*} transport missions.

Determination of transport modes and methods: In order to ensure the timely and safe forward transport and evacuation of the IO weapons and equipment {*wuqi zhuangbei*} and personnel, as well as those of the various other types of operational materiel, [the logistics support department] must flexibly apply the transport modes and methods. Transport modes include motor vehicle transport, railway {*tielu*} transport, ship/boat {*chuanting*} transport, aircraft transport, and human/animal-power {人畜力 *renchuli*} transport. The transport methods mainly include through [nonstop] transport {*zhida yunshu*}, relay transport {*jieli yunshu*}, accompanied [escorted] transport {*bansui yunshu*}, and cyclic transport {*xunhuan yunshu*}. The various methods each have their strong points, and within operations they must be flexibly selected and used {*xuanyong*}, or multiple methods applied, to carry out integrated transport {*zonghe yunshu*}.

Organization of transport safety and defense: Within future joint campaigns, in order to ensure fulfillment of the logistics transport missions, the related departments must conscientiously implement the principle of a combination of defense and strike, with defense as primary {*yifang weizhu, fangda jiehe*}; put into effect unified command of government and civilian transport, and the policy {*fangzhen*} of a tight combination of transport, repair, and defense {*yun, xiu, fang*}; and adopt multiple measures to ensure that traffic and transport lines are unimpeded. The main measures for this are as follows: first is the need to rigorously {*yanmi*} organize concealment and camouflage {*yinbi weizhuang*}, to defend against enemy reconnaissance and sabotage {*zhencha pohuai*}. Second is constructing vehicle bunkers {*yanti*}, and disposition of the necessary defensive strengths {*fangwei liliang*}. Third is doing a good job of traffic adjustment duty {*jiaotong tiaozheng qinwu*}, to preserve good transport order {*zhixu*}. **[end of page 235]**

(4) Funding support

Funding support for the joint campaign IO units is the general term for the planning, distribution {*fenpei*}, replenishment, and supply activity carried out for the funding needed by the IO units. Its main missions are as follows: to organize and implement the acquisition, supply, and management of the IO units' funding; to carry out clearing and settling of accounts {*qingli yu jiesuan*} for the funding; and to boost the funding support benefit. The logistics support department should, based on factors such as the IO missions, the real strength {*shili*} of participating personnel, the campaign duration, and the funding supply standards {*biaozhun*}, make estimates of the funding needed by the IO units; thoroughly formulate funding support plans; and, in a timely

manner and in sufficient amount {适时, 足额地 *shishi, zu'e di*}, do a good job of all funding support work. Its specific work includes the replenishment of funding and the switchover {*jiezhuan*} of the funding supply relationship, as well as funding management.

Replenishment of funding: The normal funding needed by the IO units is on a monthly basis requested {*qingling*} from higher levels by the higher-level related financial affairs departments {*caiwu bumen*}, based on the supply real strength and supply standards, and [thus] appropriated {*bofu*}. The time opportunities for funding replenishment generally are selected in the joint campaign's preparations phase and in intervals [between operations]. If critical situations arise, or if large funding payments are needed and required, and the in-advance {*shiqian*} appropriated funding moreover is not sufficient, the method of temporary {*linshi*} appropriation can be adopted to provide the support.

Switchover of the funding supply relationship: Funding switchover work must be determined based on the length of the operational duration. When the operational duration is fairly short, in principle there is no switchover of the supply relationship. When the duration is fairly long, the switching of supply {*zhuangong*} procedures can be handled per the command relationship, or the higher-level logistics will assign units {*danwei*} to carry out the switchover of supply {接供 *jiegong*}. For IO units (elements) far from organizational system units {*jianzhi danwei*}, the higher-level logistics department can assign a local unit {*jiujin budui*} to be responsible for supply. When organizational system units (elements) are moved {*diaodong*}, the organizing of funding support should be by a new supply unit relying on a letter of introduction. Funding supply for the support-the-front IO strengths relies on a real-strength voucher {实力凭证 *shili pingzheng*}, such as a letter of introduction from the local support-the-front institution or a roster {*huamingce*}, and is implemented starting on the day on which the unit receives the voucher.

Funding management: The main work of funding management includes management of funding requests, distribution, appropriation {*huabo*}, payment, and granting {*fafang*}; applications for reimbursement {*baoxiao*}; clearing and settling of accounts; and audit supervision {*shenji jiandu*}, as well as **[end of page 236]** management of valuables. Funding clearing and settling of accounts are carried out by exploiting operational intervals; are mainly based on the administrative subordination relationship {*lishu guanxi*} of supply, the funding supply standards, the higher-level-approved operational funding budget and the spending plan {*kaizhi jihua*} of the service department {*yewu bumen*}, the instructions {*pijian*} of the senior officer {*shouzhang*} responsible for payment, and the income and expense vouchers {*shouzhi pingzheng*}; and strive for daily clearing and monthly settling. In all of the links, the planning of funding, the spending, and the settling of accounts, [the logistics support department] must strengthen the audit supervision, and see that use of the funding conforms to supply standards and to the related specifications.

II. Logistics support preparations…237

The logistics support preparations for joint campaign IO are the organizational, operations-research-based planning, and other preparatory work carried out for the IO logistics support activities, in order to ensure the fulfillment of the joint campaign IO logistics support missions. Joint campaign IO logistics support is an important link in ensuring that the IO units fulfill their operational missions. The logistics support department thus must do unified operations-research-based planning considering all factors, uphold the principles, obey the laws {*guilyu*}, and in a conscientious and careful manner fully perform each task of the preparations work.

(1) Receiving the logistics support missions

The specific content in receiving logistics support missions includes the following: first is understanding the operational missions. This mainly means understanding the task organization of the IO units, and the IO missions undertaken plus the operational resolution {*zuozhan juexin*} of the IO units' senior officers, as well as the time limit for completion of the operational preparations. Second is understanding the logistics support missions. This mainly means understanding the general intent of the logistics support, the disposition of logistics support, the content and requirements of the logistics professional services support, and the time limit for completing the logistics support preparations.

(2) Collecting, analyzing, and processing logistics support intelligence information

The collection, analysis, and processing of logistics support information are important content in logistics support organization and preparations, and are the foundation and prerequisites {*qianti*} for effectively implementing IO unit logistics command, as well as for fulfilling the various support missions. Their specific content includes the following: first is collecting logistics support intelligence information. This mainly involves collecting intelligence information in respects such as the logistics supply standards, the supply real strength {*gongying shili*}, **[end of page 237]** the operational duration, the task organization and missions of the units, the current state of the logistics support strengths, the geographic environment of the operations area, and the socioeconomic situation, as well as enemy raids and sabotage {*xiji pohuai*}. The logistics department should take the initiative {*zhudong*} to maintain close contact {*miqie lianxi*} with the various other command institutions, and go through various channels to understand and grasp the situation, including the above intelligence information, the resolution of the IO commander, and the main activities of IO, as well as the needs for logistics support. Second is analyzing the logistics support intelligence information. Within the analysis process, [the logistics department] must fully consider the influence of the operational environment, the natural geographic environment, and the operations area's social environment on logistics support; capture the favorable factors and the unfavorable factors; tightly combine these with the main activities of the IO units; and

carry out qualitative and quantitative analysis, in a mutually combined manner, of the acquired intelligence information. Third is processing the logistics support intelligence information. This mainly includes carrying out sorting {*fenlei*}, filing, and analysis and processing of the logistics support intelligence information, and timely drafting of the well-processed results into the corresponding documents, to provide a basis for drafting the IO logistics support plan.

(3) Putting forth logistics support report recommendations

The joint campaign IO logistics support department should at the right time put forth logistics support report recommendations. Their main content includes the following: the logistics materiel reserves {*wuzi chubei*} and equipment serviceable rates {*wanhaolyu*} of the root-level, lower-level, and local support-the-front strengths; the current state of the logistics support strengths; the logistics support missions, plus their key points and difficult points; the organizational grouping, deployment, and mission differentiation {*renwu qufen*} of the logistics support strengths; the organization and implementation of professional services support; and the problems which require higher-level resolution.

(4) Drafting the logistics support plan

The joint campaign IO logistics support plan is the operations-research-based planning and arrangements made in advance for all items of content of logistics support. It is a component of the joint campaign IO plan, and is the basic foundation for organizing and implementing logistics support and logistics defense for the IO units. The logistics support plan usually should clarify the following: the missions and requirements of logistics support; the logistics disposition form {*bushu xingshi*}, strength organizational grouping, and mission differentiation; the reserve, allocation standards {*peibei biaozhun*}, replenishment methods, and support modes for all types of materiel; the organization and implementation methods of medical service {*weisheng qinwu*}; **[end of page 238]** the organization and implementation methods of transport service; the content and methods of coordination with friendly neighbor units {*youlin budui*} and local governments; the signal communication {*tongxin lianluo*}, warning {*jingjie*}, and defense of logistics support; and the time limit for fulfilling the missions. When drafting the logistics support plan, [the joint campaign IO logistics support department] must keep an eye on the overall situation; lay stress on the key points; fully consider all types of situations and factors, required and possible, current and following, key point and general; consider them from the [standpoint of] difficult points {*nanchu*}; and at the same time leave a certain leeway. It must, based on the IO activities COAs {*xingdong fang'an*} and on the situations which can arise, conceptualize {*gouxiang*} the logistics support COAs under various special and complex situations; and it must focus on the different situations and prepare multiple feasible COAs, so as to respond to the occurrence of various unfavorable situations.

(5) Organizing logistics support coordination

Logistics support coordination signifies the consistently adjusted-coordinated activities adopted in order to fulfill the IO logistics support missions. Organizing of logistics support coordination includes internal coordination and external coordination.

Internal coordination signifies coordination among the various departments for the IO units' logistics support, as well as among the logistics elements. Its main content includes the following: the combination of reserve, forward delivery, and rear transport for all types of logistics materiel; the linkup of transport power, and the complementation of loading and unloading; the logistics defense mission differentiation and the mutual assisting support {*xianghu zhiyuan*} of logistics defensive operations; and the coordination methods for all logistics support strengths in the different operational phases.

External coordination signifies the coordination between the logistics department and the command department {*siling bumen*}, the equipment department, the higher-level logistics department of reinforcing elements {*jiaqiang fendui*}, and the local support-the-front institution, as well as the logistics department of friendly neighbor units. Of these, the coordination with the command department mainly involves clarifying the organization of the materiel loading and unloading {*zhuangxie*} strengths, the defense and safety measures for quartermaster depots {*junxu cangku*}, and the organization of the logistics department's internal signal communication, as well as the communication methods for logistics support information. The coordination with the equipment department mainly involves clarifying the supply methods for vehicles and petroleum products, and their related instrument equipment. The coordination with the various IO units (elements) mainly involves clarifying the logistics materiel transport missions, time opportunities, and sequence {*shunxu*}; the adjusting-coordination and complementation {*xietiao peihe*} methods for forward delivery and rear transport; and **[end of page 239]** the coordinated actions {*xietong dongzuo*} of the loading, transport, and unloading links within the transport process. The coordination with attached elements mainly involves clarifying the materiel supply relationships, supply scope, and supply methods, as well as the use and differentiation of the logistics support strengths. The coordination with the local IO support-the-front strengths mainly involves clarifying the acquisition methods and settling-of-accounts procedures for local IO materiel, and the quantity, time, place, and missions for setting up {*kaishe*} of the local supply stations {*gongyingzhan*}.

Section 4: Logistics Support Implementation…240

The implementation of joint campaign IO logistics support mainly includes logistics support within situations such as marching, transport, quartering {*suying*}, and modifying the disposition, as well as executing IO missions.

I. Logistics support while on the march…240

Logistics support during marching mainly involves fuel support, quartermaster support, and medical support.

Fuel support while on the march: In order to see that the units smoothly fulfill the marching mission, the logistics department must timely organize fuel replenishment {*youliao buchong*}. Methods for fuel replenishment include the following: first is self-carrying by vehicles {*cheliang zidai*}. Each vehicle, besides filling its fuel tank, and under the premise {*qianti*} of not influencing safe operation {*anquan yunxing*}, can carry some [additional] fuel within it, for supplementary consumption {*buchong xiaohao*} at any time. Second is special-vehicle transport {*zhuanche yunshu*}. This means fixing special-vehicle transport of primary and supplemental petroleum products and of refueling instrument equipment {*jiayou qicai*}, or using tanker truck {*yunyouche*} transport, and exploiting rest stops during the march to refuel all vehicles. Third is set-point refueling {*shedian jiayou*}. This is fixed-point refueling implemented by higher levels and the root level via setting up of temporary refueling stations at appropriate points en route. Fourth is exploiting local refueling stations for refueling. This means exploiting state-owned {*guoyou*}, collective, and privately owned refueling stations en route, to carry out supplemental refueling. Fifth is air transport and air drop {*kongyun kongtou*}. This means, under special circumstances, exploiting transport planes {*yunshuji*} and helicopters to air-transport fuel, or to air-drop soft-packed fuel, to implement contingency replenishment {*yingji buchong*}. **[end of page 240]**

Quartermaster support while on the march: Well-performed quartermaster support on the marching route has an unusually important role in restoring the physical strength of personnel, and in maintaining the IO units' operational levels {*zuozhan shuiping*}. With regard to the consumption of provisions {*jiyang*} en route while on the march, usually the military service stations {*bingzhan*} and supply stations set up by higher levels or locales {*difang*} will carry out replenishment. When higher levels or locales have not set up supply stations, the problem is resolved by original organizational-system supply units {*yuan jianzhi gongying danwei*}, with the logistics department, based on the march's duration, determining whether the provisions are to be replenished. Usually when the march can be completed within two days and nights, the replenishment will be carried out after arrival at the assembly zone {*jijie diyu*}. When the march exceeds three days and nights, according to the march's agenda {*richeng*} and the units' actual situation, in-advance {*yuxian*} dispatched personnel will, at appropriate points along the way, set up provisions replenishment points (stations) {*shezhi jiyang buji dian (zhan)*}, and exploit the units' quartering time to progressively carry out replenishment.

Medical support while on the march: For the IO units' predetermined stopover zones {*tingliu diyu*}, [the logistics department] should adopt anti-epidemic measures; and for contaminated zones {*beizhanrande diyu*} or water supplies, as well as epidemic-situation areas {疫情地区 *yiqing diqu*}, it should set up markers, and guide the IO units in carrying out protection and epidemic prevention. After the units pass through

contaminated (polluted) areas/belts {*zhan (wu) ran didai*}, it must organize decontamination {*xixiao*}. The sick and wounded along the way of the units' march can be taken up {*shourong*} by take-up teams {*shourong zu*} of the various march columns {*zongdui*}, and locally {*jiujin*} sent off to on-the-way medical aid stations {*jiuhuzhan*} or wounded transfer stations {*zhuanyunzhan*} dispatched by higher levels, or to local hospitals for emergency medical treatment {*qiangjiu zhiliao*}. When necessary, [the logistics department] also can request higher levels to dispatch, or by itself dispatch treatment strengths to set up temporary medical aid stations at points which the units must cross, and carry out fixed-point reception and cure {收治 *shouzhi*} and [/or] evacuation of the sick and wounded. For advance elements {*xianqian fendui*}, vanguard elements {*qianwei fendui*}, or units (elements) marching along independent routes, it should reinforce them with certain medical strengths. When the IO units run into an enemy raid and experience fairly many wounded, besides organizing the units' self and mutual aid {*zijiu yu hujiu*}, it also should unfold some medical strengths to carry out the rescue/first-aid {*qiangjiu*} work, wait until arrival at a high-level medical treatment institution, and then turn over the wounded personnel and swiftly rejoin their unit {*guidui*}.

II. Logistics support during transportation…241

The main activities steps of transportation include loading, movement {*yunxing*}, and unloading. Within the loading process, the main content of logistics support includes the following: based on needs and requirements, setting up medical aid stations, refueling stations, and drinking-water supply stations within the loading zone; constructing the necessary simple living facilities; **[end of page 241]** and organizing personnel to request loading instrument equipment. Within the movement process, when the movement time is fairly long, [the logistics department] should provide the units with the requisite quartermaster support, such as food and drinking water. Within the unloading process, due to facing a fairly high enemy threat, the situation will be complex and the facilities equipment will be simple and crude {*jianlou*}, so it must strengthen organization and command, and support the IO units in completing the unloading and moving in {*kaijin*} toward the assembly zone in a swift, concealed, and safe manner.

III. Logistics support within quartering…242

Quartering is temporary accommodation {*linshi zhusu*} while units are on the march or within the process of carrying out various missions. Its goal is to see that the IO units obtain rest and reorganization, so that they can better complete the march and other missions. When IO units are organizing quartering, the main content of the logistics support work includes the following: the first is swiftly understanding the attrition and loss {*xiaohao, sunshi*} situation of all types of materiel within the unit maneuver {*budui jidong*} process, and adopting the method of a mutual combination of forward delivery and self-obtaining {*ziling*}, to provide replenishment. Second is as rapidly as possible unfolding the units' medical treatment strengths, to receive, treat, and evacuate the wounded, and to organize medical treatment teams {*yiliao zu*} to conduct [doctors']

rounds {*xunzhen*}. Third is organizing repair {*xiuli*} strengths to assist the units (elements) in overhauling {*jianxiu*} the vehicles. Fourth is dispatching personnel to inspect and guide the units in the food and drink support and sanitation situation in the quartering area, and in timely adopting the corresponding measures. When the quartering zone encounters an enemy raid, [the logistics department] should swiftly organize strengths to rescue the wounded, and assist the units (elements) in repairing from the aftermath of the raid {*xiaochu xiji houguo*}.

IV. Logistics support when modifying the disposition…242

Logistics support for the IO units when modifying the disposition must, based on the different situations of disposition modification, actively adopt the corresponding support measures. When an IO unit while modifying the disposition suffers an enemy ground firepower strike, and the IO unit completely halts its activities and relies on favorable terrain to resist the enemy attack {*jingong*}, the logistics department then should swiftly readjust the strengths, and concentrate all its power on supporting the resistance activities, right until the enemy's offensive intention {*jingong qitu*} is crushed. When only a part of the IO unit halts the activities of modifying the disposition and shifts into resistance, and the remaining greater part continues to readjust the disposition {*tiaozheng bushu*}, the logistics department then should, based on the instructions of the IO unit commander, **[end of page 242]** use one part of the strengths to support the unit's resistance activities, while having the remaining strengths follow the IO strengths modifying the disposition to carry out the readjustment. When an IO unit within the process of modifying the disposition encounters an enemy small-band force-strength harassing attack {*xiaogu bingli xirao*}, the unit should organize warning force-strengths to respond to it, while the main-force unit continues to modify the disposition; and the logistics department then should dispatch some force-strengths to support and screen the warning force-strengths' activities, while most of the logistics strengths will follow the main force to carry out the readjustment or shift. When an IO unit within modifying of the disposition suffers an enemy raid by air cannon firepower {空炮火力 *kongpao huoli*} or NBC weapons, the logistics commander should swiftly understand the unit's casualties and losses situation, organize rescue, and carry out materiel replenishment. When an IO unit suffers an enemy NBC raid and the unit suspends modifying of the disposition, logistics should swiftly organize strengths to assist the unit in repairing from the aftermath of the raid.

V. Logistics support during execution of IO missions…243

Within the process of the IO units' execution of the IO missions, the main work of logistics support is as follows: first is organizing materiel replenishment. This mainly uses forms such as planned replenishment {*jihua buji*}, ad hoc replenishment {*suiji buji*}, and emergency replenishment {*jinji buji*}, to carry out timely replenishment of units carrying out IO missions. Second is organizing and guiding food and drink support. The logistics strengths should, based on the battlefield situation, guide the IO units in adopting the corresponding field [open-air] cooking {*yechui*} form, and carrying out hot-

food preparation. When food and drink preparation for first-line units is difficult, [the logistics department] should organize rear support strengths to carry out assisting support {*zhiyuan*}, to ensure their needs and requirements. Third is organizing and guiding materiel management. Within the process of the IO units' execution of missions, logistics, besides properly conducting depot materiel management, should place the key points on guiding the IO units in doing a good job of light materiel {*qingzhuang wuzi*} management, organizing the units in retrieving battlefield-abandoned materiel, and properly organizing the exploitation of battlefield-captured {战利缴获 *zhanli jiaohuo*} logistics materiel. Fourth is at the right time readjusting the logistics strengths. When the battlefield situation undergoes change, and the original deployment zones are no longer convenient for implementing support, the IO units' logistics strengths should at the right time readjust the disposition, organize depot transfer {*cangku zhuanyi*}, and swiftly unfold the work. When the logistics support strengths encounter sabotage and are unable to implement support, the logistics department should in good time readjust the use of the logistics strengths, to swiftly restore the support capability. **[end of page 243; end of chapter]**

This page intentionally left blank.

Chapter 13
Joint Campaign Information Operations Equipment Support…244

Joint campaign information operations (IO) equipment support {*zhuangbei baozhang*} indicates the general term for the various supportive measures adopted, and corresponding activity {*huodong*} carried out within joint campaigns, in order to maintain and restore the good technical status [configuration] {*jishu zhuangtai*} of the IO weapons and equipment {*wuqi zhuangbei*}, and is an important component {*zucheng bufen*} of joint campaign equipment support.[11] Its basic missions are as follows: under the assisting support {*zhiyuan*} of the higher-level equipment support strengths {*liliang*}, to do unified operations-research-based planning {*tongchou*} for use of the IO equipment support strengths within the task organization of campaign {*zhanyi biancheng*}, and of those from high-level reinforcement {*jiaqiang*} and mobilization {*dongyuan*}; mainly via four support forms {形式 *xingshi*}, organizational system {*jianzhi*}, base {*jidi*}, support-the-front {*zhiqian*}, and rear {*houfang*}, to implement equipment and materiel {*zhuangbei wuzi*} support, technical support, equipment management, and equipment funding {*jingfei*} support for IO; and to support the smooth fulfillment of the joint campaign IO missions {*renwu*}.

Section 1: Equipment Support Requirements {*yaoqiu*}…244

Following on the day-by-day rise in the position {*diwei*} of joint campaign IO, the quantities of IO equipment are growing ever greater and its technical content is growing ever greater; and the degree of sharpness of information warfare [IW] {*xinxi duikang*} is constantly increasing. The position of IO equipment support similarly is becoming ever more important, and its role {*zuoyong*} ever more prominent; these have thus put forth even more stringent requirements on organizing and implementing IO equipment support. **[end of page 244]**

I. Full preparations, active initiative {*jiji zhudong*}…245

Full preparations are the basis for seizing the initiative, and are a prerequisite {*qianti*} for smoothly fulfilling the equipment support missions. The full-process quality {*quanchengxing*} of joint campaign IO requires that the equipment support institution {*jigou*} not only must before combat fully do well in all preparations for IO equipment support, become familiar with the various equipment support preliminary courses of action [COAs] {*yu'an*}, implement various readiness {*zhanbei*} measures, strengthen the foresight quality {*yujianxing*} of equipment support, thoroughly formulate support plans

[11] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

{*jihua*}, and complete all preparations work before the commencement of operations, but also must actively do well in the sustained {*chixu*} support preparations for the IO units {*budui*} of all participating services and arm {*canzhande ge junbingzhong*} and for the local support-the-front {*difang zhiqian*} IO strengths. The equipment support institution should, under the premise {*qianti*} of not going against the operational intent {*zuozhan yitu*} and not influencing the overall situation {*quanju*} of equipment support, give the lower levels the authority {权力 *quanli*} for discretionary handling {机断处置 *jiduan chuzhi*}, fully bring into play their subjective dynamic quality {*zhuguan nengdongxing*}, and see that they fulfill the support missions in a manner with active initiative and creativity.

II. Synthetic application {*zonghe yunyong*}, unified command {*tongyi zhihui*}…245

Synthetically applying various equipment support strengths and implementing unified command are the keys to smoothly accomplishing joint campaign IO equipment support. In future joint campaign IO, the enemy and friendly sides {*diwo shuangfang*} both will employ a variety of IO strengths to contend for information superiority {*zhengduo xinxi youshi*} in all fields, land, sea, air, and space {*lu, hai, kong, tian*}, with synchronous conduct of joint campaign information offense {*xinxi jingong*} and information defense {*xinxi fangyu*}, and with alternating employment of information means such as electronic attack {*dianzi jingong*}, network attack {*wangluo gongji*}, and force-strength and firepower strikes. These traits {*texing*} of defense within attack {*gongzhong youfang*}, attack within defense {*fangzhong yougong*}, integration of attack and defense {*gongfang yiti*}, and mutual supplementation {相辅相成 *xiangfu xiangcheng*} have determined that the equipment support institution is a synthesis {*zongheti*}, composed of many systems {*xitong*}, many departments, many classes {*zhonglei*}, and many professions {*zhuanye*}, and that the support strengths' internal and external coordination relationships {*neiwai xietong guanxi*} are complex. Hence, the joint campaign IO equipment support institution must synthetically apply a variety of equipment support strengths, and implement unified command, to bring into play the effectiveness {*xiaoneng*} of integrated-whole {*zhengti*} support. In particular, when supporting the main operational activities {*zuozhan xingdong*}, it must break through traditional professional bounds, and synthetically apply various support strengths to establish an integrated support network system of systems [SoS] {*zonghe baozhang wangluo tixi*} with front and rear linked up {*qianhou xianjie*} and left and right interconnected {*zuoyou xianglian*}, and with longitudinal radiation {*zongxiang fushe*} and lateral linkup {*hengxiang guantong*}, so that between the armed forces and the local [strengths], among all services and arms, **[end of page 245]** and among all professions, an organic support integrated whole is formed, and so as to put into effect concentrated employment {*jizhong shiyong*} and unified command of the various support strengths, consistently adjusted-coordinated {*xietiao*} to fulfill the equipment support missions.

III. Class-by-class implementation {*fenlei shishi*}, mutual supplementation {*huwei buchong*}…246

Within joint campaigns, adoption of the methods of class-by-class implementation and mutual supplementation for IO equipment support is an important measure for smoothly fulfilling the joint campaign [IO] equipment support missions. In joint campaign IO, the participating strengths are many, and the weapons and equipment involved can be summed up as mainly dividing into two classes {*lei*}: the first is firepower lethal-quality weapons {*huoli shashangxing wuqi*}. These weapons mainly undertake defensive missions {*danfu fangweixing renwu*} within joint campaign IO, and in terms compared to IO equipment they mainly are light weapons. The second is the IO weapons and equipment, mainly including electronic warfare [EW] {*dianzi duikang*} equipment, network warfare {*wangluo duikang*} equipment, and special IW {*teshu xinxizhan*} weapons and equipment. These weapons and equipment of different systems {*tizhi*} and different categories {*leibie*} can from the equipment technology standpoint be divided into two classes: professional and nonprofessional. Within past operations, the armed forces' technical support for traditional weaponry and facilities equipment {*bingqi shebei*} amassed a good deal of valuable experience, and established a relatively perfect support system {*tizhi*}. However, support for professional IO weaponry technology still is a blank space. The joint campaign IO equipment support institution can only be completed by relying on peacetime research and training {*yanjiu, xunlian*} and on wartime trial and error {*mosuo*}. Hence, within joint campaign IO, in order to even better accomplish the support missions, the joint campaign IO equipment support institution should carry out differentiation {*qufen*} of the support missions for equipment technology; i.e., class-by-class implementation of nonprofessional equipment technical support and professional equipment technical support, organizing of two sets of different support strengths, formulating correlated plans {*xiangguan jihua*}, setting the support resolution {*dingxia baozhang juexin*}, and, under unified command by a joint campaign IO commander {*zhihuiyuan*}, jointly fulfilling the operational support missions. However, within specific {*juti*} operational processes, the two should, based on the specific operational support mission, supplement one another {*xianghu buchong*} and mutually coordinate {*huwei xietong*}, to ensure the smooth fulfillment of the joint campaign IO missions. **[end of page 246]**

IV. Forward employment {*kaoqian shiyong*}, support key points {*zhongdian*}…247

Within joint campaigns under modern conditions, IO equipment will successively or simultaneously encounter the enemy's soft and hard kill {*ruanying shashang*}. Not only will the equipment damage {*sunhuai*} be severe, but also the damage mechanisms {*sunhuai jili*} will be complex. They not only can be expressed as software faults {*ruanjian guzhang*} in the equipment, but also can be expressed as hardware damage to the equipment; and they not only can be expressed as systems being out of order and [/or] paralyzed {*shiling, tanhuan*}, but also can be expressed as systems unable to operate {*caozuo*} or scrapped {*baofei*}. In order to support the timely repair {*xiufu*} of joint campaign IO weapons and equipment, only when the equipment support strengths are

forward employed near the deployment {*peizhi*} of the objects {*duixiang*} of support can they shorten the support distance, improve the support time effectiveness {时效 *shixiao*}, and be able to obtain effective screening {*yanhu*} by the units, which is beneficial to safety. Forward employment of the support strengths must lay stress on the support key points, use the main strengths in the main direction {*zhuyao fangxiang*}, for the main units, in important areas {*diqu*}, for the key point equipment, in the critical time segments {*guanjian shijie*}, and in the key point links {*huanjie*}, so as to ensure fulfillment of the main mission.

V. Strengthening defense {*fangwei*}, ensuring safety…247

Strengthening the self-defense {*zishen fangwei*} of the joint campaign IO equipment support institution and ensuring the safety of the units are conditions for fulfilling the joint campaign IO equipment support missions. In future joint campaigns, the IO units will conduct maneuvering {*jidong*} within a fairly large scope. The equipment support strengths certainly will conduct activity in the full depth {*quan zongshen*} of the battlefield; their distribution will be large in area, the fluid quality {*liudongxing*} of personnel will be high, and they will face the threat of the enemy's hard and soft dual strike. On one hand, since the IO equipment support strengths mostly accompany the IO units to implement the support, the opportunities for contact with the enemy are increased, and they are subject to direct threats from enemy force-strengths and firepower. On the other hand, since the IO equipment support institution's self-defense strengths are thin, and it usually carries out support missions under adverse battlefield environmental conditions, its survivability {*shengcun nengli*} is greatly reduced. Hence, the joint campaign command institution {*zhihui jigou*} should bring the defense of the equipment support institution into the rear defense operational plan {*houfang fangwei zuozhan jihua*}, with its implementation under unified organization by the joint campaign command {*zhihuibu*}. The equipment support institution must boost its own defensive capability; establish the thought of active defense {*jiji fangwei*}; and, via methods such as flexible organizational grouping {*linghuo bianzu*}, decentralized deployment {*shusan peizhi*}, rigorous camouflage {*yanmi weizhuang*}, and timely maneuver, boost **[end of page 247]** battlefield survivability.

VI. Combination of military and civilians {*junmin jiehe*}, integrated {*yiti*} support…248

In future joint campaign IO, the participating strengths will be multidimensional {*canzhan liliang duoyuan*}. They not only will include the IO units of all services and arms, but also will include the local IO assisting-support strengths. Hence, the IO equipment support missions will be strenuous, and only relying on the armed forces' organizational system support strengths will pose difficulty in being equal to the task. [We] must develop the superiority of people's war {*renmin zhanzheng*}, and tightly rely on the assisting support of the local governments and the masses. The joint campaign IO equipment support institution on one hand must grasp the situation of the operations area's {*zuozhan diqu*} local repair and technical personnel, machine and tool facilities

equipment {*jiju shebei*}, and general-purpose instrument equipment reserve {*qicai chubei*}. On the other hand, it should establish a set of rapid and effective mobilization mechanisms, and, based on the local support-the-front capability, rationally commandeer [its strengths]. At the same time, it also must bring the mobilized support-the-front strengths and materiel and instrument equipment {*wuzi qicai*} into the unit equipment support SoS, and fully bring into play military-civilian integrated-whole might {*junmin zhengti weili*}, to joint support the IO units' operations.

Section 2: Organizational Grouping and Disposition {*bushu*} of Equipment Support Strengths…248

I. Organizational grouping of equipment support strengths…248

The organizational grouping of joint campaign IO equipment support strengths is the temporary-quality combination {*linshixing zuhe*} carried out with the IO equipment support strengths as the basis. Its goal {*mudi*} is to see that the existing equipment support strengths form a powerful equipment support composite strength {*heli*}, to bring into play their optimum benefit. Usually it is determined by taking the existing strengths for IO equipment support as the basis, according to the quality and quantity of the root unit's equipment technical personnel, and the reality of wartime equipment support.

The joint campaign IO equipment support strengths usually have a task organization [composed] of equipment support strengths from higher-level reinforcement and the root-level organizational system, the local accompanying support-the-front {*difang suijun zhiqian*} equipment support strengths, and the equipment support strengths of the attached units (elements) {*peishu bu (fen) dui*} from higher-level reinforcement. Usually **[end of page 248]** organizational grouping is rationally carried out by adopting a mutual combination of the equipment support technical department's equipment technical personnel and element {*fendui*} equipment technical personnel, and a mutual combination of technical mainstays and general technical personnel, with the key points on supporting the needs and requirements {*xuyao*} of the groupings and elements {*qun, dui*} in the main operational direction and undertaking the main mission. Also, adopting the method of a mutual combination of fixed-point-support organizational grouping and mobile-support {*jidong baozhang*} organizational grouping [enables] doing well in the equipment support work for all IO units (elements). Fixed-point-support organizational grouping involves, on the basis of the original technical strengths, and based on the needs and requirements for reinforcing certain technical strengths, composing equipment support small elements {*xiao fendui*}, responsible for the equipment support missions of the root grouping (sub-grouping) {*qun (fenqun)*}. Mobile-support organizational grouping is the equipment technical support work of organizing mobile equipment support small elements and various units (elements) for mobile assisting support {*jidong zhiyuan*}.

II. Disposition of equipment support strengths…249

The joint campaign IO equipment support disposition signifies the differentiation, organizational grouping, and deployment of the joint campaign IO equipment support strengths. Correct disposition of the joint campaign IO equipment support strengths is the basis for establishing an integral {*wanzheng*} and stable equipment support SoS, and for smoothly fulfilling the joint campaign IO equipment support missions. The joint campaign IO equipment support disposition, serving as an important component of the operational disposition {*zuozhan bushu*}, should be determined based on the resolution of the joint campaign IO commander and on the IO units' operational activities, as well as the battlefield environment.

According to the basic requirements for the joint campaign IO equipment support disposition, the dispositional forms of the IO equipment support strengths mainly are as follows: the first is the grouped (area/zone) disposition {*chengjituan (quyu) bushu*}. Usually this is used under circumstances where the battlespace {*zhanchang kongjian*} is fairly small and relatively fixed, and where the terrain and road conditions are fairly good. Second is the echeloned disposition {*chengtici bushu*}. Usually this is used when the operational disposition depth is fairly large, when restricted by the enemy situation {*diqing*} and by roads and terrain, and when the grouped disposition is not convenient for support. Third is the per-direction disposition {*anfangxiang bushu*}. Usually this is used when the operational front {*zhengmian*} is fairly large and when terrain and road conditions are poor and not convenient for centralized {*jizhong*} support. Fourth is the per-direction echeloned disposition {*anfangxiang chengtici bushu*}. This contains the common traits of the per-direction and echeloned dispositions, and is relatively suitable for use when the IO units **[end of page 249]** are rapidly maneuvering. At actual application time, the above several dispositional forms should be flexibly applied, based on the battlefield's specific situation.

The basic requirements for the joint campaign IO equipment support disposition are as follows: first is that it must be mutually adapted to the IO disposition, with the main support strengths placed in the main IO direction. Second is that it must be linked up {*xianjie*} with the higher- and lower-level equipment support disposition. It must, based on the battlefield terrain conditions and the location of the objects of support, take the roads as axes, to compose a deep-disposition {*zongshen tici*} support SoS with proper distances, a clear division of labor, and front and rear linked up, to fully bring into play the role of the IO support institutions at all levels. Third is that it must be mutually adjusted-coordinated with the logistics disposition {*houqin bushu*}. For the convenience of coordination and boosting of integrated-whole support efficiency {*xiaolyu*}, the IO commander must take all things into consideration {*tongpan kaolyu*} in the disposition of the logistics and equipment support strengths. Fourth is that it must be mutually combined with the local support-the-front strengths. The local support-the-front strengths must be used as a part of the equipment support strengths, with unified planning {*tongyi jihua*}, unified organization, and unified employment, to bring into play the role of military-civilian integrated-whole support.

Section 3: Equipment Professional Services {*zhuanye qinwu*} Support and Preparations…250

The joint campaign command institution should, based on factors {*yinsu*} such as the missions and circumstances {形势 *xingshi*} of IO, the operational duration {*chixu shijian*}, the classes and quantities of participating equipment, and the allocated {*diaopei*} support capability, organize equipment professional services support and preparations.

I. Professional services support…250

Professional services support for joint campaign IO equipment mainly includes equipment materiel support, equipment technical support, equipment management, and equipment funding support.

(1) Equipment materiel support

Joint campaign IO equipment materiel support signifies the general term for the acquisition {*choucuo*}, reserve {*chubei*}, replenishment {*buji*}, and management activity [conducted] for the spare parts {*lingbeijian*} used in maintenance {*weixiu*} of the IO equipment and instrument equipment. **[end of page 250]** It is the basis for carrying out the IO missions, and also is an important component of joint campaign equipment support. The joint campaign command institution should, based on factors such as the missions and circumstances of IO, the operational duration, the classes and quantities of participating equipment, and the support capability, respectively make estimates {*yuji*} of the needs and requirements loads {*xuyaoliang*} for the IO reconnaissance {*zhencha*}, information systems protection {*xinxi xitong fanghu*}, and information offense equipment; thoroughly formulate equipment support plans; and, according to the principles of laying stress on key points, full complements of systems {*xitong peitao*}, appropriate quantities, and convenience for allocation and transport {*diaoyun*}, in good time fully carry out all IO equipment materiel support work tasks. Its main missions include the following:

Equipment materiel reserve {*wuzi chubei*}: The joint campaign IO equipment materiel reserve is the foundation on which the IO units maintain combat power {*zhandouli*}. When carrying out joint campaign IO equipment materiel reserve, [the joint campaign command institution] must emphasize fully grasping the following several links: the first is to control the quantity of equipment materiel reserve. The reserve quantity of IO equipment materiel is mainly determined based on the IO missions, the quantities of the various types of IO equipment, the operational duration, the degree of difficulty in replenishment {*buchong*} during combat, and the storage conditions. This reserve quantity should be able to support the needs and requirements of at least a single campaign (battle) in one phase of war. In the war's early period, the main direction should be able to support the needs and requirements of three campaigns (battles), and a general direction should be able to support the needs and requirements of one or two

campaigns (battles). Second is that the equipment materiel reserve must have comprehensive full complements {*zonghe peitao*}. It requires giving comprehensive consideration, according to unified planning, to the varieties, quantities, and specifications {*guige*} of the materiel needed for IO, and achieving completeness of varieties, moderateness in quantity, fullness of specifications, and guarantee of both quality and quantity {*baozhi baoliang*}, so as to form an integrated-whole quality {*zhengtixing*} in IO equipment materiel support. Special-project instrument equipment {*zhuanxiang qicai*} must have a fully complemented reserve according to the unit standards {基数标准 *jishu biaozhun*} for the various models {各型 *gexing*} of IO equipment maintenance instrument equipment {*zhuangbei weixiu qicai*}. Self-made parts and fittings {*lingpeijian*} also must be fully complemented {配齐 *peiqi*} per standards. Third is that the reserve of equipment materiel must lay stress on key points. The key points of joint campaign IO equipment materiel reserve should be the materiel, instrument equipment, and facilities equipment whose information technology [IT] {*xinxi jishu*} content is high. For some IT facilities equipment with a high IT content and which China cannot produce, and thus must be procured {*caigou*} from abroad, it is even more important to increase the reserve portion {*chubei fen'e*}. The IO materiel, instrument equipment, and facilities equipment for the armed forces' special purposes should **[end of page 251]** be obtained from the armed forces' reserves, while military-civilian general purpose materiel, instrument equipment, and facilities equipment should as much as possible be obtained from the reserves of the local related departments or institutions. Fourth is that the equipment materiel reserve must be arranged {*buju*} rationally. [The joint campaign command institution] should comprehensively consider factors such as the operational missions and disposition of the IO units, and the terrain, road, and storage conditions within the operations area, as well as the deployment of the local equipment departments, to see that all support links of the IO units are mutually linked up, to form an IO maintenance instrument equipment support net of deep echelons {*zongshen tici*} and also having key points, higher and lower [levels] linked up, and left and right interconnected.

Equipment material replenishment {*buji*}: Joint campaign IO equipment materiel usually is replenished per the administrative subordination relationship {*lishu guanxi*}; i.e., replenishment is carried out per the systems {*xitong*} of the joint campaign command and of the equipment departments of the various operational groups (groupings) {*zuozhan jituan (qun)*}. To do well in equipment materiel replenishment, three aspects should be given attention: the first is the replenishment time opportunities {时机 *shiji*}. Usually this involves exploiting favorable time opportunities such as times of unit assembly {*jijie*} and holding {*daiji*}; intervals between operational phases; and [occasions] when we have seized local air dominance/supremacy {*jubu zhikongquan*}, crushed the enemy raids {*xiji*}, penetrated the enemy defense, and achieved encirclement {*hewei*} of the enemy and pursuit and annihilation {*zhuijian*} of the fleeing {*kuitao*} enemy, as well as exploiting darkness and poor weather such as foggy days. The second is the replenishment method. IO equipment materiel replenishment, according to requirements for being at the right time, in the right place, in the right amount, and being applicable {*shishi, shidi, shiliang, shiyong*}, and based on the actual needs and requirements and the

equipment support possibility, usually is flexibly organized and implemented by adopting a mutual combination of level-by-level replenishment {*zhuji buchong*}, bypassing replenishment {*yueji buchong*}, and mutually regulated replenishment {*huxiang tiaoji buchong*}, with level-by-level replenishment as primary; a mutual combination of higher-level planned replenishment and lower-level requests, with higher-level planned replenishment as primary; a mutual combination of higher-level forward delivery {*qiansong*} and lower-level pickup {*lingqu*}, with higher-level forward delivery as primary; according to the sequence {*shunxu*} of first in the main operational direction and then in the other operational directions, first for the main operational units and then for the other operational units, and first for the urgently needed IO equipment and instrument equipment and then for routine equipment and instrument equipment. Third is the replenishment form. This can adopt the fixed-point, accompanied {*bansui*}, and follow-up {*genjin*} modes. Fixed-point replenishment is replenishment carried out for IO units via materiel and instrument equipment storehouses {*cangku*}, field {*yezhan*} materiel and instrument equipment storehouses, and materiel and instrument equipment replenishment stations {*bujizhan*}, as well as by exploiting rear bases, integrated equipment storehouses {*zonghe zhuangbei cangku*}, and military service stations {*bingzhan*} storing maintenance instrument equipment. Accompanied replenishment is mostly used for replenishment of IO units while they are maneuvering. Follow-up replenishment is mostly used for replenishment of IO units when the maneuvering speed {*jidong sudu*} is fairly rapid and the maneuvering distance {*jidong juli*} **[end of page 252]** is fairly long.

(2) Equipment technical support

Joint campaign IO equipment technical support signifies the technical measures adopted in order to maintain {*weihu*} and restore the tactical technical characteristics {*jishu zhanshu xingneng*} of the IO equipment and to preserve IO capability. [The joint campaign command institution] should, based on factors such as the campaign pattern {*zhanyi yangshi*}, the IO missions, the duration, the classes and quantities of the participating equipment, the technical situation, the employment intensity {*shiyong qiangdu*}, the protection conditions, the equipment technical support capability, the enemy's strike means, and the possible degree of sabotage {*pohuai chengdu*}, as well as the operations area's natural geographic conditions, make scientific estimates of the equipment damage level {*sunhuailiang*}, damage degree {*sunhuai chengdu*}, repair mission load {*xiuli renwuliang*}, and the maintenance instrument equipment needs and requirements load; thoroughly formulate IO equipment technical support plans; and in a timely and high-efficiency manner properly carry out the technical support work for all types of IO equipment. Its main missions include the following:

The equipment damage rate {*sunhuailyu*} estimate is an estimate made for the equipment damage degree in a single operation. Its goal is to provide a basis for formulating equipment support plans, for arranging the repair missions, for preparing the maintenance instrument equipment, and for differentiating and using the repair strengths. The factors influencing equipment damage are quite numerous, so when estimating,

[command institution personnel] should synthetically [comprehensively] analyze {*zonghe fenxi*} the specific situation of each operation, and reference the empirical data {*jingyun shuju*} from past similar operations, to as much as possible see that the estimate approaches the real-combat damage rate {*shizhan sunhuailyu*}. On the basis of estimating the equipment damage rate and damage degree, they can estimate the maintenance mission load for the damage grades {*sunhuai dengji*} of all types of IO equipment, and, based on the mission differentiation {*renwu qufen*} of all maintenance institutions, calculate the corresponding maintenance mission load. Estimates of the equipment maintenance missions should synthetically apply various estimation methods, to as much as possible make relatively accurate estimates.

The equipment repair modes according to organizational form are divided into on-the-spot repair {*xiandi xiuli*} and evacuation for repair {*housong xiuli*}. On-the-spot repair is a commonly used repair mode, and includes positional repair {*zhendi xiuli*}, circuit repair {*xunhui xiuli*}, and accompanied repair {*bansui xiuli*}. Within operations, all combat-loss equipment {*zhansun zhuangbei*} which can be given on-the-spot repair — and in particular, equipment with a fairly great influence on combat power — should as much as possible be repaired on the spot. To this end, the repair institutions should be forward deployed {*kaoqian peizhi*}, and the repair strengths should have a level-by-level projection {逐级前伸 *zhuji qianshen*}, for key point reinforcement {*zhongdian jiaqiang*}. At the same time, **[end of page 253]** based on the operational missions of the IO units (elements), the repair capability, and the quantity and degree of equipment damage, [the repair institutions should] adopt different repair methods, to as rapidly as possible restore the technical performance of the damaged equipment, and boost the "regeneration" {*"zaisheng"*} capability of the equipment. Within the operational process, damaged equipment, and in particular equipment with a medium and heavy degree of damage, cannot completely get repaired on the spot or in the root-level repair institution. It should be withdrawn from its position {*chechu zhendi*}, relatively concentrated in a fairly safe place, and then evacuated for repair.

Equipment rescue and repair {*qiangjiu xiufu*} are important means for making up for operational losses, for supplementing {*buchong*} combat real strength {*zhandou shili*}, and for preserving the capability for sustained operations {*chixu zuozhan nengli*}. In organizing and implementing wartime equipment rescue and repair, first is formulating realistic {*qieshi kexing*} rush repairs COAs {*qiangxiu fang'an*}. [The command institution] must timely grasp the IO equipment damage situation, and, based on the specific situation, formulate realistic rush repairs COAs and properly carry out full material {*wuzhi*} preparations, to ensure the ability at any time to execute rush repairs missions. Second is scientifically applying the rush repairs strengths. It generally adopts the methods of a mutual combination of IO equipment department personnel and element {*fendui*} technical personnel, a mutual combination of technical mainstays and general mainstays, a mutual combination of local technical personnel and unit technical personnel, and a mutual combination of higher-level [dispatched] reinforcing technical personnel and IO unit personnel. At the same time, it should strengthen contacts with local governments and plants, understand the situation of their facilities equipment and

technical strengths, and establish cooperative relationships, to facilitate obtaining their assistance during rush repairs. Third is synthetically applying multiple repair methods. [This adopts] a mutual combination of fixed-point repair and mobile assisting-support repair {*jidong zhiyuan xiuli*}, with fixed-point repair as primary, and a mutual combination of replacement-part repair {*huanjian xiuli*}, repair via cannibalization (of parts) {*chaipin xiuli*}, and original-part repair {*yuanjian xiuli*}, with replacement-part repair as primary; [operates] first on the easy [repairs] and then the difficult, first on the light and then on the heavy, and first on the critical positions {*guanjian buwei*} and then on the general positions; [works] first on the main direction and then on the secondary direction; and [adopts] a mutual combination of professional repair personnel, operating use {*caozuo shiyong*} personnel, and local assisting-support personnel, with the professional repair personnel as primary. Fourth is doing everything possible for on-the-spot, fastest-possible repair {*jiudi jinkuai xiufu*} of damaged and faulty {*sunshang, guzhang*} equipment; and when it cannot be repaired, [the command institution] should immediately organize evacuation for repair.

(3) Equipment management

The technical quality {*jishuxing*} of joint campaign IO equipment is strong, which [places] **[end of page 254]** stringent requirements on the weather conditions, such as clearing of clouds {阴晴 *yinqing*}, rain and fog, and dry and wet cold and heat {*ganshi lengre*}. In particular, under conditions of terrain such as plateaus, high and cold areas, deserts, and gobi [i.e., Gobi Desert-like areas], the fault rate {*guzhanglyu*} of equipment increases, and its operating performance {*shiyong xingneng*} markedly decreases. When organizing IO equipment management, [the command institution] must specially formulate an upkeep system {*baoyang zhidu*} for wartime IO equipment, and see that the equipment's tactical technical characteristics {战技性能 *zhan ji xingneng*} from start to finish are kept in the optimum status; it must differentiate the key points {*huafen zhongdian*}, for class-by-class implementation {*fenlei shishi*}; and it must combine these with the characteristics {*tedian*} of IO equipment, and thus formulate specific management measures. Before entering the operations area, it must focus on the different natural geographic environmental characteristics; based on the technical requirements for equipment operating management {*shiyong guanli*}, conduct all-around inspections of the participating equipment; and in advance do a good job of all preparations, to boost the adaptability {*shiyingxing*} of the equipment to the natural environment. After entering the operations area, it must, based on the battlefield equipment operating/use situation, as rapidly as possible revise the rules and regulations {*guizhang zhidu*} for equipment handover {*jiaojie*}, management, and inspection, to guard against equipment loss and damage; it must strengthen equipment parking installations {*tingfang sheshi*} and facilities equipment building {*shebei jianshe*}, and improve the storage and safekeeping {*baoguan*} conditions, to boost management standards {*shuiping*}; and it must strengthen defense, protection, and maintenance, to detect faults and promptly eliminate them, and to boost the serviceable rate {*wanhaolyu*} of the participating equipment.

(4) Equipment funding support

The main missions of joint campaign IO equipment funding support are to organize and implement the acquisition, supply {*gongying*}, and management of equipment funding, and to carry out clearing and settling of accounts {*qingli yu jiesuan*} for equipment funding. In organizing equipment funding support, [the command institution] should, based on factors such as the joint campaign IO missions, the equipment real strength and conditions, the intensity and duration of IO, and the classes and quantities of participating equipment, as well as the funding supply standards {*gongying biaozhun*}, scientifically evaluate-appraise {*pinggu*} the IO equipment funding needs {*xuqiu*}; thoroughly formulate IO equipment funding support plans; and adopt effective modes to promptly appropriate {*bofu*} the funding, strengthen funding management, and properly carry out the IO equipment funding support work.

II. Equipment support preparations…255

Joint campaign IO equipment support is the foundation for and a prerequisite for implementing IO. The work is extremely complex. It requires paying a high degree of attention, and in a thorough and careful manner properly performing **[end of page 255]** all preparatory work for IO equipment support, especially the professional services support work, to ensure the smooth conduct of joint campaign IO.

The equipment support preparations work for joint campaign IO mainly includes the following: collecting, analyzing, and processing intelligence information; putting forth equipment support recommendations; drafting {*nizhi*} equipment support plans; and organizing equipment support coordination. The joint campaign IO equipment support institution must in a thorough and carefully way properly carry out all preparatory work for IO equipment support.

(1) Collecting, analyzing, and processing intelligence information

Collecting intelligence information: The content of collecting IO equipment support intelligence information mainly includes the following: the basic situation of IO equipment; its employment and storage situation; the situation of fault repair or preventive maintenance {*yufangxing weixiu*} within the processes of use and storage; the reliability {*kekaoxing*} and maintainability {*weixiuxing*} data for components and parts {*lingbujian*}; the spare parts and other supply varieties, needs, and consumption {*xiaohao*} quantities; the budget and actual expenses and receipts {*shouzhi*} for equipment use and maintenance; and information in respects such as the equipment support institutions, facilities equipment, and installations for the various types of IO units.

Analyzing intelligence information: On the basis of grasping the information, [the joint campaign IO equipment support institution] conducts a basic analysis and assessment {*fenxi panduan*} of the current support situation. This mainly includes the

following: the units {*danwei*} and equipment for current key point support, whether the time opportunities for materiel replenishment are suitable {*qiadang*}, the support modes and methods which should be used, and whether the support strengths need to be adjusted.

Processing intelligence information: The procedures {*chengxu*} and methods for the processing of IO equipment support information include the following: first are examination {*shencha*} and screening {*shaixuan*}. Examining and screening the integrity {*wanzhengxing*} and accuracy {*zhunquexing*} of the information requires again providing or rejecting equipment support information which does not conform to requirements; and it requires carrying out supplementation {*buchong*} for a lack of critical equipment support information. When there are information items missing supplementation {漏填 *loutian*} and also difficult to supplement fully {补齐 *buqi*}, the necessary technical processing should be carried out. Second are sorting {*fenlei*} and priority setting {*paixu*}. [This means] carrying out sorting of the collected raw information, such as dividing it into equipment use information, repair information, and instrument equipment information. Third are statistics and calculations. From large quantities of data **[end of page 256]** statistics and calculated results, the IO equipment technical situation and development trends can be seen. Fourth is analysis and assessment. On the basis of the above work, and taking the IO equipment support decision-making objectives {*juece mubiao*} and the related instructions {*zhiling*} and equipment support standards {*biaozhun*} as the foundation, [the joint campaign IO equipment support institution] determines the output {*shuchu*} content, flow direction {*liuxiang*}, mode, and time requirements for the equipment support information. After collecting, analyzing, and processing the IO units' equipment support information and intelligence, it should draft the information into textual {*wenzishi*} or graphical {*tubiaoshi*} documents, and report them to higher-level commanders or issue them to the units.

(2) Putting forth equipment support recommendations

The joint campaign IO equipment support department should at the right time put forth equipment support report recommendations {*baogao jianyi*}. Their main content includes the following: the equipment support strengths' dispositional pattern; the task organization, mission differentiation, and deployment of the equipment support institution; the organization of communication and defense; the employment differentiation and protection for the forward transport and rear transport {*qianyun houyun*} roads; the preparations standards and depletion norms {*xiaohao xian'e*} for the maintenance instrument equipment; the time limit for completing preparations for support; and the problems which need high-level resolution.

(3) Drafting equipment support plans

The IO equipment support organ {*jiguan*} should — based on the operational intent of the IO commander, the operational orders, and the operational plans, as well as the instructions and requirements for equipment support work, the higher-level

equipment support instructions, the quantity and quality {*shuzhiliang*} and thought situation of the IO units' equipment support element personnel, the strength task organization, the quantity and quality of the equipment, the needs and supply possibility for rush repairs and for munitions {*danyao*} and maintenance instrument equipment, and the operations area's weather, terrain, roads, water sources, and other exploitable resources — consider all things, and thoroughly draft the support plans.

The content of joint campaign IO equipment support plans usually includes the following: the mission differentiation, personnel organizational grouping, deployment requirements, and support modes for the equipment support strengths; the equipment's combat loss rate {*zhansunlyu*} estimate, and the measures for rescue, rush repairs, and evacuation, as well as upkeep; the depletion norms for the maintenance instrument equipment and munitions; the related specifications {*guiding*} for equipment support coordination, signal communication {*tongxin lianluo*}, and defense; the supply and reserve of instrument equipment; the methods for the equipment's servicing inspection {*weihu jiancha*} and rush repairs; **[end of page 257]** and the time limit for completing the preparations.

(4) Organizing equipment support coordination

Joint campaign IO equipment support coordination is the adjusting-coordination activity carried out, per equipment support plans, for the interior and exterior of the IO equipment system {*xitong*} and among the support activities. Its goals are to achieve consistent adjusting-coordination with the joint campaign equipment support activities, and to fully bring into play integrated-whole support functions {*gongneng*}.

External coordination: IO equipment support's external coordination signifies the coordination between the joint campaign IO equipment support command institution and the root-level operational command institutions, political departments, logistics command institutions, friendly neighbor unit {*youlin budui*} equipment support institutions, and the local support-the-front institutions.

Internal coordination: The coordination for the IO equipment support's interior signifies the planned and adjusted-coordinated activity carried out in order to maintain the mutual adjusting-coordination and unified [nature] of the IO equipment command institution's internal support activities, so that all service departments {*yewu bumen*} and support units form an integrated-whole support composite strength {*zhengti baozhang heli*}, and fulfill the fixed IO unit equipment support missions. Internal coordination includes the following: coordination of the entire system, coordination among the service departments, and coordination of equipment support defense.

Section 4: Equipment Support Implementation…258

The implementing of joint campaign IO equipment support should place the key points on properly organizing equipment support for the main activities, including IO reconnaissance, information offense, and information defense.

I. Equipment support for IO reconnaissance activities…258

Equipment support for IO reconnaissance activities should take support for the various types of IO reconnaissance equipment as key points, and in good time organize the IO reconnaissance equipment's reserve, **[end of page 258]** allocation and supply {*diaobo gongying*}, replenishment {*buchong*}, and technical support, as well as management. It is generally implemented per the organizational system's system {*jianzhi xitong*}. Due to the weakness of the IO reconnaissance equipment's defensive capability, it is susceptible to the enemy's strikes and sabotage; so [this type of equipment support] should exploit the integrated-whole defensive strengths in order to enhance protection for this equipment. When the equipment encounters strikes or sabotage, [the joint campaign IO equipment support command institution] should timely organize strengths to as much as possible implement rescue and rush repairs in a local and convenient manner {*jiujin jiubian di*}. When the equipment damage is severe and cannot be repaired, it should in good time organize strengths to carry out equipment replenishment, so as to ensure the fulfillment of the IO reconnaissance missions.

II. Equipment support for information offense activities…259

Equipment support for information offense activities should take as key points the IO units (elements) which undertake the main information offense missions. [This involves] timely understanding the main objectives of the information offense activities, and the offensive means adopted, as well as the quantity, class(es), and intensity of the employed force-strengths, and at the right time changing the key points of IO equipment support, and adjusting the support COAs and support strengths.

When conducting electronic jamming {*dianzi ganrao*} and electronic deception {*dianzi qipian*} against the enemy, [the equipment support command institution] should take as the support key points the soft-strike equipment, such as that for active jamming {*youyuan ganrao*}, passive jamming {*wuyuan ganrao*}, and computer virus attack {*jisuanji bingdu gongji*}; appropriately adjust the support strength organizational grouping; differentiate the objects of support; clarify the support missions; and swiftly dispatch strengths to implement forward support for the units (elements) conducting electronic jamming and electronic deception in the campaign's important phases or time segments, main directions, and key point areas.

When executing hard destruction {*ying cuihui*} against the enemy, [the equipment support command institution] should, based on the joint campaign IO plans, take as the support key points the hard-destruction equipment, such as anti-radiation weapons

{*fanfushe wuqi*} and directed energy weapons [DEWs] {*dingxiang neng wuqi*}. Before the operational activities commence, it should dispatch support strengths to the units for timely replenishment {*buchong*}, servicing, and repair of their various types of equipment, and to assist the units in doing well in the preparations. During the operational activities, it should timely grasp the equipment's depletion and damage situation, at the right time organize replenishment {*buji*}, and promptly repair the damaged equipment. When necessary, it can dispatch support strengths to implement on-the-spot support or accompanied support.

When executing computer network attack against the enemy, [the equipment support command institution] should at the right time provide the commander with technical recommendations on infiltrating {*shentou*} and sabotaging the enemy computer networks. When executing computer virus attack, **[end of page 259]** it should timely put forth technical recommendations in respects such as what virus to employ and how to implant it into enemy systems, and organize strengths to properly provide the necessary technical support.

III. Equipment support for information defense activities…260

Equipment support for information defense activities should take the communication nets, radar nets, and computer nets as the support key points.

Equipment support when countering the enemy's reconnaissance and electronic jamming: [The equipment support command institution] should timely adopt measures to service and repair the various types of electronic equipment {*dianzi zhuangbei*}; replenish the units' urgently needed technical instrument equipment for irising {*zheguang*}, noise silencing {*xiaosheng*}, and electromagnetic [EM] shielding {*dianci pingbi*}; put forth the related technical recommendations; strictly control EM radiation {*dianci fushe*}; cut down on the information transmission load {*xinxi chuanshuliang*}; and defend against enemy jamming and sabotage of our information systems, so as to support the safety and stability of the information systems' operation.

[Equipment] support when defending against enemy computer network attack: [The equipment support command institution] should place the key points on strengthening the security management {*anquan guanli*} for computer networks, and on strict computer operating specifications {*shiyong guiding*}; and it should timely replace the (secret) keys {*miyao*}, construct network firewalls {*wangluo fanghuoqiang*}, and implement uninterrupted monitoring {不间断监测 *bujianduan jiance*} of the operating state {*gongzuo zhuangtai*} of computer networks, to defend against the enemy's execution of infiltration and attack against our computer networks. Also, it must focus on the characteristics and adopted means of enemy-executed attack, and constantly research the corresponding protection methods and measures.

Equipment support when resisting the enemy's entity destruction {*shiti cuihui*} of our information systems: [The equipment support command institution] should take as

the [support] key points our command centers, communication hubs {*tongxin shuniu*}, radar stations, and computer network nodes {*jisuanji wangluo jiedian*}, and timely organize supply support for electronic camouflage instrument equipment {*dianzi weizhuang qicai*} and other protective instrument equipment. When necessary, it can reinforce some IO equipment support strengths, while at the same time other strengths will jointly support the IO units' maneuver, decentralization {*shusan*}, and concealment {*yinbi*}. After suffering an enemy strike, it should swiftly organize the support strengths for IO equipment and systems, effect rush repairs to damaged IO equipment, promptly restore operation {*yunxing*} of the systems, and at the right time replenish damaged information equipment and correlated instrument equipment. **[end of page 260; end of chapter]**

This page intentionally left blank.

Chapter 14
Joint Campaign Information Operations Political Work…261

Joint campaign information operations (IO) political work is the thought work and organizational work carried out, within the entire process of organizing and implementing IO, under the unified leadership of the Party committee of the joint campaign command {*lianhe zhanyi zhihuibu*}, for the participating IO units {*canzhande xinxi zuozhan budui*} and local support-the-front personnel {*difang zhiqian renyuan*}, as well as the propaganda offensive {*gongshi*} and psychological disintegration work carried out against the enemy. Political work within joint campaign IO is an important assurance of strengthening the Party's leadership over the operations, preserving the highly centralized and unified {*jizhong tongyi*} [nature] of the IO units {*budui*}, maintaining {*weihu*} internal and external unity {*tuanjie*}, consolidating and boosting unit combat power {*zhandouli*}, fully bringing into play the integrated-whole operational might {*zhengti zuozhan weili*} of people's war {*renmin zhanzheng*} and joint campaigns, and gaining success in IO.

Section 1: The Missions of Political Work…261

Within joint campaign IO, the Party committees and political organs {*jiguan*} at all levels must, based on the joint campaign operational intent {*zuozhan yitu*} and the operational missions {*zuozhan renwu*} of the IO units, launch {*kaizhan*} powerful political work in a timely and high-efficiency manner. Its main missions are as follows:

I. Unifying the thought of the officers and men {*guanbing*}…261

[This means] resolutely implementing and executing the joint-campaign-related concept of operations [ConOps] {*zuozhan fangzhen*} and instructions {*zhishi*} of the Party Central Committee and the Central Military Commission [CMC] {*zhongyang junwei*}, **[end of page 261]** unifying the units' awareness of the justness {*zhengyixing*} and lawfulness {*hefaxing*} of operations, enhancing the officers' and men's sense of responsibility for safeguarding national sovereignty and territorial integrity, and firmly believing in the correct command of the Party Central Committee and CMC. [It means] unifying the IO units' understanding of the operational goals {*zuozhan mudi*} and operational thought, and consciously seeing that military activities {*xingdong*} are mutually complemented by national political, diplomatic, and legal struggle {*douzheng*}. [It means] unifying the awareness of operational discipline and policy specifications, educating the officers and men in fully understanding the special quality {*teshuxing*} of IO and the complexity of the operational environment, and achieving strict enforcement of orders and prohibitions {令行禁止 *lingxing jinzhi*} and unimpeded flow of military and government orders {*junling zhengling*}.

II. Inspiring the fighting will of the officers and men…262

[This means] educating and guiding {*yindao*} the officers and men in gaining a clear understanding of the nature of joint campaigns and the superiority of our military; establishing the firm resolve of fighting to safeguard national reunification {*weihu zuguo tongyi*}, fighting for the fundamental interests of the Chinese nation, and fighting for national dignity; and strengthening the conviction in certain victory in a just war. [It means] arousing the participating officers' and men's spirit of a high degree of patriotism and revolutionary heroism, and strengthening the units' confidence and courage in the certain victory of those who dare to strike {敢打必胜 *ganda bisheng*}. [It means] guiding the units in combining a courageous spirit with a scientific attitude, closely pressing {*jintie*} the IO units to launch military democracy, constantly innovating fighting methods {*zhanfa*}, fully bringing into play the intelligence and wisdom of the numerous officers and men, and working hard to seize success in operations at minimum cost.

III. Ensuring the centralized unified [nature]…262

[This means] upholding the Party committee's unified leadership of IO, and ensuring the smooth implementation of joint campaign IO in terms of thought, in terms of organization, and in terms of the laws and regulations system {*fagui zhidu*}. [It means] educating the units in establishing political consciousness, consciousness of the big picture {*daju yishi*}, and the concept of joint gaining of victory {*lianhe zhisheng guannian*}; correctly handling the relationship of the integrated whole {*zhengti*} to its parts {*jubu*}, and that of the main direction {*zhuyao fangxiang*} to the secondary direction; and [establishing] active complementation {*jiji peihe*} and initiative-based coordination {*zhudong xietong*}. [It means] upholding the Party committee's collective decision-making {*jiti juece*} for major issues, timely bringing into play the active quality {*jijixing*} of the senior officer's division of labor and personal responsibility {*shouzhang fengong fuze*}, and properly using ad hoc handling authority {*linji chuzhiquan*}. [It means] timely adjusting and replenishing {*tiaozheng buchong*} all levels and all types of {*geji gelei*} of cadres in the IO units; placing the key points {*zhongdian*} on properly complementing the leadership teams {*banzi*} at all levels and the professional and technical personnel {*zhuanye jishu renyuan*} urgently needed for operations; and attaching importance to bringing into play the cohesive role {*ningju zuoyong*} of Party and [Youth] League organizations {*dangtuan zuzhi*} at all levels. [It means] conscientiously implementing the principles and laws {*fagui*} of joint campaign IO, and educating the units in strictly executing the coordination plan {*xietong jihua*} and resolutely **[end of page 262]** submitting to unified command {*tongyi zhihui*}.

IV. Bringing into play the might of people's war…263

[This means] actively complementing the local Party committees and governments in doing a good job of political mobilization, guiding the masses {*qunzhong*} in gaining a clear understanding of the position and role {*diwei zuoyong*} of joint campaigns, arousing the masses' enthusiasm for supporting the army and being

patriotic {拥军爱国 *yongjun aiguo*} and for participating in supporting the front {*canzhan zhiqian*}, maintaining the armed forces' internal and external unity {*tuanjie*}, and bringing into play the might of people's war. [It means,] based on the IO needs and requirements {*xuyao*}, adjusting-coordinating the theater's {*xietiao zhanqu*} local Party committees and governments in ably carrying out the work of science and technology [S&T] supporting the front {*keji zhiqian*}, information supporting the front, talent supporting the front, and supporting the army and giving preferential treatment to soldiers' families {拥军优属 *yongjun youshu*}. [It means] organizing and launching joint defense {*lianfang*} to counter infiltration {*fanshentou*}, counter psychological warfare [PSYWAR] {*fanxinzhan*}, counter incitement to defection {*fancefan*}, and counter theft of secrets {*fanqiemi*}, and strengthening the concept of the masses defending against an enemy situation of harassing attacks {*xiraode diqing*}, to ensure the safety and social stability of our important information targets {*xinxi mubiao*}.

Section 2: The Requirements {*yaoqiu*} for Political Work…263

The unfolding {*zhankai*} of joint campaign IO before other operational activities, and its penetration through the entire process {*quancheng*} of operations, have put forth new and even more stringent requirements on political work.

I. High-technical content and smartness levels {*zhinenghua chengdu*} in IO weapons and equipment necessitate bringing into play the intelligence and wisdom of the participating officers and men…263

Following on the breakthrough-quality development of computer technology {*jisuanji jishu*} and artificial intelligence [AI] {*rengong zhineng*} methods and their application in the military, the knowledge {*zhishi*} content and technical content of future joint campaign IO are growing ever larger, and its smartness level is growing ever higher. This requires that IO personnel must be alert and resourceful {*jimin*} in reaction, have a solid foundation in training {*xunlian yousu*}, be proficient in technology, and be conscientious in work, so as to fulfill multiple arduous missions. To this end, joint campaign IO political work on one hand must regard realizing the optimum combination of men and technical equipment as the focus of attention {*zhuoyandian*} in the work, and educate the officers and men in establishing a scientific and rigorous work attitude, combining a courageous spirit with a scientific attitude, and correctly using and skillfully operating the various types of weapons and technical equipment, to fully bring into play their operational effectiveness {*zuozhan xiaoneng*}. **[end of page 263]** On the other hand, [political work] must attach importance to doing well in the thought work for the technical experts and the critical-post technical personnel, fully bring into play their intelligence and wisdom and subjective dynamic quality {*zhuguan nengdongxing*}, and to the maximum extent arouse {*diaodong*} their operational enthusiasm {*zuozhan jijixing*} and creativity.

II. The tightness of IO attack and defense combination {*gongfang jiehe jinmi*} and the stringent requirements on integration {*yitihua*} necessitate bringing into play military-civilian {*junmin*} integrated-whole operational might…264

Joint campaign IO has an integrated quality {*yitixing*} in the IO platforms, the IO activities, the various strike means, and the operational space {*zuozhan kongjian*}. How to unify and adjust-coordinate all participating strengths and the various operational means, so that their superiorities are complementary {*youshi hubu*} and so that they form an integrated-whole operational composite strength {*zhengti zuozhan heli*}, just have become the keys to IO. To this end, first is the need to bring into play the cohesive function {*ningju gongneng*}, so that there is mutual assisting support {*huxiang zhiyuan*}, mutual supplementation {*huxiang buchong*}, and coordinated operations {*xietong zuozhan*} among all operational strengths {*zuozhan liliang*}, the various operational means, all operational spaces, the IO systems {*xitong*}, and the operational activities, and so that they become an organic integrated whole. Second is the need to educate the units in firmly establishing the concept of integrated-whole operations and the concept of coordinated operations, and promoting fraternal unity {*tuanjie you'ai*} and the spirit of sacrificial dedication, for the benefit of the integrated whole and the overall situation {*quanju*}, and sparing no sacrifice for the overall situation benefit. Third is the need to educate the units in strictly executing the coordination specifications, taking initiative for complementation {*zhudong peihe*}, closely coordinating, and fully bringing into play the integrated-whole operational might of people's war under modern conditions.

III. The strong time effectiveness quality {*shixiaoxing*} of IO and the sharpness of confrontational tension {*duikang jinzhang*} necessitate bringing into play the rapid reaction capability of political work…264

Future joint campaign IO will have a rapid tempo {*jiezou*} and a strong time effectiveness quality; the battlefield situations will be intricate and complex {*cuozong fuza*}, and opportunities for combat {*zhanji*} will be fleeting {稍纵即逝 *shaozong jishi*}. This requires that information activity must be timely, reliable, and highly efficient. In particular, in joint campaign IO under complex electromagnetic [EM] environments {*dianci huanjing*}, at all times {*meishi meike*} there will always be large quantities of information flowing. Within these, the fictitious will be mixed with the genuine {鱼目混杂 *yumu hunza*}, the true will be difficult to distinguish from the false {真假难辨 *zhenjia nanbian*}, and information transmission and processing {*xinxi chuandi he chuli*} will be faced with very great difficulties. Whether [we] can within a limited time accurately acquire, transmit, process, and employ information will become the key to the success or failure of joint campaign IO. To this end, first is the need to educate the units in a high degree of concentration in terms of spirit and always striving to do better {精益求精 *jingyi qiujing*} in technical terms, excelling at **[end of page 264]** seizing and exploiting opportunities for combat, and seizing the initiative {*zhudongquan*} in IO, to create the conditions for all campaign operations. Second is the need to enhance the time effectiveness quality and directed [focused] quality {*zhenduixing*} of political work; work hard to accomplish rapid detection of problems, rapid information transmission, and

rapid resolution of problems; neither wait for nor be reliant [on others' aid] {不等不靠 *budeng bukao*}; and act promptly at one's own discretion {机断行事 *jiduan xingshi*}. Third is that the messages and instructions {*wendian, zhishi*} of political work must be brief and to the point {*jianming eyao*}; the launching of agitprop must be brief and forceful, and emphasize practical results {讲求实效 *jiangqiu shixiao*}; and the organizational grouping {*bianzu*} of political organ strengths must be highly efficient and elite {*gaoxiao jinggan*}, with all service departments {*yewu bumen*} adjusted-coordinated consistently. Fourth is the need to tightly center on operational reality; launch mass agitprop work; organically combine thought education, organization of cohesion, and law and discipline constraints {*faji yueshu*}; and see that the political work infiltrates {*shentou*} into the midst of all technical service work.

IV. The unfolding of IO before other campaign activities and its penetration from start to finish of campaign operations necessitate the Party committee's full-process leadership…265

Joint campaign IO has a long duration {*chixu shijian*}, involves all fields {*lingyu*} of joint campaign operations, and penetrates from the start to the finish of joint campaign operations, all of which has put forth even more stringent requirements on joint campaign IO. To this end, political work must ensure the Party committee's full-process leadership of operations, to ensure the realization of the Party committee's operational intent and the satisfactory fulfillment of the operational missions. First is the need to organize the units in conscientiously studying {*xuexi*} the strategic concept {*zhanlue fangzhen*} of the Party Central Committee and CMC, correctly recognizing and understanding the joint campaign IO-related concept and principles of the Party Central Committee and CMC, and using the orders and instructions of the Party Central Committee and CMC to unify the units' thought. Second is the need to fully bring into play the cohesive role of Party committees at all levels, the combat bastion {*zhandou baolei*} role of the [Party] branches, and the exemplary role played {*mofan daitou zuoyong*} by Communist Party members. Third is the need to guide the units in availing themselves of every opportunity {见缝插针地 *jianfeng chazhendi*} to launch agitprop work and in timely transmitting the orders and instructions of the Party Central Committee and CMC and of the higher levels, and to educate the units in developing the fighting spirit {*zhandou jingshen*} of continuous operations {*lianxu zuozhan*} and of courage and tenaciousness, and all along preserving high combat morale.

V. The enemy's strength and our weakness {敌优我劣 *diyou wolie*} in IO weapons and equipment necessitate educating the units in being grounded in existing equipment, and in the firm confidence in the certain victory of those who dare to strike…265

Joint campaign IO, just in terms of weapons and technical equipment, as compared to the powerful enemy, [**end of page 265]** is overall [a situation of] the enemy's strength and our weakness. To this end, [we] must educate the units in fully understanding the important position of joint campaign IO, in being grounded in

operations with the existing technical equipment, and in establishing confidence in using inferior equipment to defeat an enemy with superior equipment. On one hand, [we] must educate the units in dialectically regarding the strong points of the weapons and equipment, and see that the officers and men understand that even though {*jinguan*} the enemy's high-tech weapons and equipment have their strong points, nonetheless they also have vulnerabilities {*cuiruo*} and "soft ribs." Provided that we fully bring into play the subjective dynamic quality of the men, exploit favorable factors {*yinsu*} such as climate and topographical advantages {天时, 地利 *tianshi, dili*} and the support of the people {*renhe*}, bring into play the strong points of our IO weapons and equipment, and attack the enemy's weak points, we are fully capable of defeating the powerful enemy. On the other hand, [we] must educate the units in fully bringing into play military democracy, actively exploring {*jiji tansuo*}, creating IO strategies and tactics having our military's characteristics, adopting the correct operational stratagems {*moulue*} and methods, and constantly summarizing and perfecting within practice.

Section 3: The Political Work of the Operational Preparations Phase…266

In joint campaign IO, the peacetime-wartime demarcation line {*pingzhan jiexian*} is blurred, the imminent battle training {*linzhan xunlian*} time is pressing and its requirements stringent, and the main threads {*touxu*} of the preparations work are numerous. Political work must make the best use of the limited time before imminent battles {*linzhan*}; carry out in-depth and meticulous, and solid and effective thought work and organizational work for the units; and ensure that the peacetime to wartime transition work is timely, fast, and highly efficient.

I. Widely and deeply carrying out political mobilization and propaganda and education…266

First of all, [the Party committees and political organs] should clarify the goals, significance, and missions of joint campaign IO, and encourage the officers and men to establish a sense of the sacred mission and sense of honor in fighting to safeguard homeland security {*baowei zuguo anquan*}, for the great cause of national unification {*minzu tongyi*}, and for the fundamental interests of the people. Next, they must impress on the IO units the reality of thought {*sixiang shiji*} and the operational missions undertaken {*danfu*}, timely put forth agitprop slogans, correct the attitude of participating personnel toward operations, and ensure that the officers and men from start to finish maintain a high combat morale. Third, they [must] in depth carry out education in readiness for the circumstances {形势战备 *xingshi zhanbei*}; strengthen the officers' and men's enemy situation concept {*diqing guannian*}, **[end of page 266]** readiness concept, and secrecy concept {*baomi guannian*}; and educate the units in an on-duty system {*zhiban zhidu*} of strict readiness, early warning, and forecast {*yubao*}, so that the units maintain vigilance at all times {常备不懈 *changbei buxie*}. Finally, [they must] educate the units in correctly understanding the enemy and friendly strength comparison {*diwo liliang duibi*}, in dialectically analyzing the favorable conditions and unfavorable factors in the enemy and friendly sides' operations, in scientifically grasping the relationship

between men and weapons within modern war, in overcoming the psychology of fear and cowardice in fighting {怯战 *qiezhan*}, and in strengthening the confidence in the certain victory for those who dare to strike.

II. Establishing and perfecting all levels of Party and Youth League organizations and their mass organizations {*qunzhongxing zuzhi*}…267

First is that [the Party committees and political organs] should attach the fullest importance to strengthening the building {*jianshe*} of the subordinate units' Party and Youth League organizations and of other soldiers' organizations {*junren zuzhi*}, and fully bring into play the core role and cohesive role of Party organizations at all levels. Second is that they should conduct education of the subordinate units in respect to organizing discipline, strengthen the Party's policy and discipline {*zhengce jilyu*} propaganda, and elevate the concept of policy and discipline for the entire body of participating personnel. Third is that they should timely allocate {*diaopei*} and replenish the cadres, place the key points on evenly allocating and mandatorily allocating {配齐, 配强 *peiqi, peiqiang*} the IO units' leadership teams at all levels and their important-post technical personnel, and establish a wartime cadre deputy system {*dailiren zhidu*} and cadre reserve courses of action [COAs] {*chubei fang'an*}. Fourth is that they should widely launch meritorious-service encouragement and reward activity {*ligong jiangli huodong*}, formulate and declare wartime meritorious-service standards, and encourage the units' spirit of revolutionary heroism.

III. Organizing and launching military democracy, boosting the units' tactical and technical levels {*zhanji shuiping*}…267

Based on the operational missions undertaken by the units, [the Party committees and political organs] on one hand must guide the subordinate units in launching mass pre-combat S&T troop training activity {*keji lianbing huodong*} in a manner having a directed [focused] quality {*you zhenduixing di*}; organize the officers and men in analyzing the enemy and friendly operational posture {*diwo zuozhan taishi*}, handling difficulties, coming up with measures, seeking countermeasures, and discussing fighting methods; unify the units' operational thought; and perfect the operational COAs {*zuozhan fang'an*}. On the other hand, they must focus on the technical difficult points which can be encountered within joint campaign IO; mobilize {*fadong*} experts, scholars, and professional and technical personnel in scientific research and colleges and schools {*yuanxiao*} in launching technical brainstorm projects {*jishu gongguan*} and in creating new fighting methods; educate the officers and men in combining explanations of technology and of tactics together with the battle of wits and battle of courage {斗智与斗勇 *douzhi yu douyong*} against the enemy; and timely summarize and disseminate the new experience and new fighting methods created by the units within practice.

IV. Doing well in the work of anti-spying protection of secrets {*fangjian baomi*} and of safeguarding of security {*anquan baowei*}…267

[The Party committees and political organs] should, based on the higher levels' concept, policy, and instructions for safeguarding {*baowei*} work, organize the units **[end of page 267]** in carrying out the work of anti-spying protection of secrets and of safeguarding of security. First is rigorously {*yanmi*} organizing the units in launching mass anti-spying {*fangjian*}, counter-espionage {*fante*}, counter-theft-of-secrets {*fanqiemi*}, and counter-PSYWAR {*fanxinzhan*} activity, and educating the participating units in constantly maintaining a high degree of political vigilance {*jingtixing*} and strictly defending against the enemy's various types of sabotage activity {*pohuai huodong*}. Second is strengthening revolutionary-integrity and anti-corruption education, firmly laying the thought foundation for defending against the enemy's PSYWAR and incitement to defection {*xinzhan, cefan*}. Third is educating the units in strictly guarding military secrets, strictly executing secrecy specifications {*baomi guiding*}, and ensuring the safety of secrets carriers {*mimi zaiti anquan*}. Fourth is strict political examination {*shencha*} work for personnel at vital sites and key point positions {*yaohai, zhongdian buwei*}, to ensure security and warning {*anquan jingjie*} for command organs {*zhihui jiguan*} and important targets {*mubiao*}. Fifth is actively launching "three warfares" {*"sanzhan"*} activity; based on the correlated policy and laws {*falyu*}, applying various modes to actively conduct policy and laws and regulations {*zhengce fagui*} education and anti-PSYWAR education for participating personnel and the masses; and conducting propaganda on the war goals and significance, revealing the enemy's crimes, and stabilizing the troops' morale {*junxin*}.

Section 4: The Political Work of the Operational Implementation Phase…268

In joint campaign IO, the battlefield situation is fast changing {*shunxu wanbian*}, the enemy and friendly confrontation is unusually sharp, and the pressure bearing on the psychology of the officers and men is high. The [corresponding] political work must tightly fix on the operational progress {*zuozhan jincheng*}, focus on the different operational activities, and adopt various forms {形式 *xingshi*} to bolster the high combat morale of the officers and men and to support {*baozhang*} the fulfillment of the joint campaign IO missions.

I. Political work within IO reconnaissance {*xinxi zuozhan zhencha*}…268

The effective implementation of IO reconnaissance enables timely and accurately grasping the enemy's disposition {*bushu*} and operational intention {*zuozhan qitu*}, and provides intelligence support {*qingbao baozhang*} to all levels of commanders {*zhihuiyuan*} for carrying out correct decision-making and for command of operational activities. In political work within IO reconnaissance, first is the need for timely and ably performing the thought work for IO reconnaissance unit personnel, and in particular for the computer network experts {*jisuanji wangluo zhuanjia*} and important technical personnel: seeing that they fully understand the important meaning of IO reconnaissance,

clarifying the operational goals and missions, and fully bringing into play the subjective dynamic quality of operations by numerous officers and men. **[end of page 268]** Second is encouraging them to scrupulously discharge their duties {恪尽职守 *kejin zhishou*} and be courageous in operations, and, with a high degree of awareness of responsibility, consummate technique {*jingzhan jishu*}, and flexible tactics {*linghuode zhanshu*}, use all ways and means {千方百计地 *qianfang baiji di*} to acquire the location, categories {*leibie*}, and tactical and technical parameters {*zhanjishu canshu*} of the enemy information targets. Third is focusing on the difficult problems encountered within information reconnaissance activities, fully bringing into play military democracy, and widely mobilizing {*fadong*} technical experts and technical personnel to research new fighting methods for vanquishing the enemy {*kedi zhisheng*}. Fourth is guiding the units in devoting particular care to struggle tactics {*douzheng celue*}, combining discussions of technology and discussions of tactics together with the battle of wits and battle of courage, and adopting multiple modes and multiple means to satisfactorily accomplish the IO reconnaissance missions.

II. Political work within information offense {*xinxi jingong*} activities…269

In political work within information offense, first is the need to educate the units in carrying forward the revolutionary heroism spirit of daring to fight and risk one's life {敢打敢拼 *ganda ganpin*} and fighting decisive battles for decisive victory [determining to fight and win] {*juezhan juesheng*}, and in adopting multiple means and methods, [such as] having defense within attack {*gongzhong youfang*}, to resolutely seize and maintain the initiative within joint campaign IO. Second is the need to educate the officers and men in combining the revolutionary spirit together with a scientific attitude; persisting in handling matters according to scientific laws {*guilyu*}; accomplishing conscientiousness in responsibility, scientific high efficiency, and always striving to do better {*jingyi qiujing*}; and realizing the optimum combination of men and technical equipment. Third is educating the units in establishing coordinated operations, the concept of composite strength to gain victory {*heli zhisheng*}, and initiative-based complementation {*zhudong peihe*} and mutual assisting support; effecting close complementation {*jinmi peihe*} between all IO units and the local information assisting-support strengths, and among all operational activities; and coordinating activities, to ensure the bringing into play of our integrated-whole IO effectiveness {*zhengti xinxi zuozhan xiaoneng*}. Fourth is organizing and guiding {*zhidao*} the units in fully applying the technical equipment superiority of the IO units, and at the right time launching a psychological propaganda offensive {*xinli xuanchuan gongshi*} against the enemy, to disintegrate the will to fight in the enemy officers and men, and accelerate the progress of victory in the war.

III. Political work within information defense {*xinxi fangyu*}…269

In political work within information defense activities, first is the need to educate the IO units in fully recognizing the important meaning of information defense activities; establishing the thought of military-civilian integrated-whole protection {*junmin zhengti fanghu*} and integrated operations {*yiti zuozhan*}; from start to finish adopting combat

enthusiasm-laden active information defense {*jijide xinxi fangyu*} activities, and [adopting] a dauntless revolutionary heroism spirit which is heroic and indomitable and does not fear sacrifice; and launching full-process protective operations in a vigilant and flexible, neither bending nor swerving manner {机警灵活, 不屈不挠地 *jijing linghuo, buqu bunao di*}. Second is focusing on **[end of page 269]** the operational activities which can be adopted in an enemy information attack {*xinxi gongji*}, and educating the officers and men in the need for active initiative {*jiji zhudongdi*} in properly carrying out the various technical, tactical, and psychological protective measures to defend against and overcome the psychology of passive waiting {*xiaoji dengdai*}, tension, panic, and fear. Third is organizing the units in launching mass battlefield agitprop work; and when meeting with the enemy's long-range precision guided munitions [PGM] {*yuancheng jingque zhidao wuqi*} and network attacks and psychological attacks, they must timely and properly carry out the thought work for the battlefield officers and men, as well as the theater masses {*zhanqu qunzhong*}, to stabilize their morale {*qingxu*}. Fourth is educating the units in boosting the awareness of camouflage {*weizhuang*} and protection, strictly observing battlefield discipline, and consciously maintaining battlefield order {*zhixu*}.

IV. Political work within information security [INFOSEC] secrecy {*xinxi anquan baomi*}…270

In political work within INFOSEC secrecy, first is the need to educate the officers and men in overcoming lack of confidence {*weinan qingxu*}, at all times maintaining a high degree of political vigilance, starting out by oneself, strictly guarding military secrets, and strictly executing secrecy specifications, to ensure the safety of our secrets carriers. Second is strengthening the revolutionary-integrity and anti-corruption education of the officers and men, and firmly laying the thought foundation for the officers and men to defend against the enemy's PSYWAR and incitement to defection. Third is strengthening leadership, and perfecting the organizations; guiding the units in launching mass anti-spying, counter-espionage, and counter-theft-of-secrets activity, activity to strictly defend against the enemy's various types of theft of secrets and sabotage, and strict political examination work for personnel at vital sites and key point positions; and strengthening security and warning {*anquan jingjie*} for the head organs {*shounao jiguan*} and important targets. Fourth is adopting strict protection and countermeasures {*fangfan cuoshi*} for important information carriers, such as those related to plans and orders, and for important cleared personnel {涉密人员 *shemi renyuan*}; strictly controlling the dissemination scope and mode for important information; and as much as possible reducing the scope of access to secrets {知密范围 *zhimi fanwei*} on operational information, and shortening the time of access to secrets. Fifth is strengthening the control {*guanzhi*} and examination work for wartime news and propaganda and communication and correspondence {*tongxin xinjian*}, and defending against leaks of secrets {*xiemi*} by the newspaper and magazine, radio, TV, and other news media and by communication and correspondence. Sixth is educating operational and technical personnel in taking good care of technical equipment, strictly operating {*caozuo*} per rules and regulations {*guizhang*} and per technical requirements and norms, and to the

maximum extent preventing and [/or] reducing the giving away of secrets {失密 *shimi*} and leak of secrets caused by technical faults and by mistakes in technical operation {*jishu caozuo shiwu*}. **[end of page 270; end of chapter]**

This page intentionally left blank.

Chapter 15
Information Operations in a Joint Fire Strike Campaign…271

Joint fire strikes are a series of fire assault {*huoli tuji*} activities conducted by concentrating employment {*jizhong shiyong*} of Second Artillery Corps conventional missile units {*changgui daodan budui*}, and Air Force as well as Navy and Army long-range strike strengths {*yuancheng daji liliang*} against the enemy's important targets {*mubiao*}. Information operations [IO] serve as important operational activities {*zuozhan xingdong*} for blocking and sabotaging {*zuduan, pohuai*} the enemy's information acquisition, processing, and transmission {*xinxi huoqu, chuli he chuanshu*} channels, and for ensuring friendly {*jifang*} information and information system security {*xinxi xitong anquan*}; and their role within joint fire strikes is becoming more prominent every day. The main missions of joint fire strike campaign IO are as follows: to organize and conduct IO reconnaissance {*zhencha*}, with the key points {*zhongdian*} on ascertaining the situation of the composition, deployment {*peizhi*}, and technical parameters {*canshu*} of the enemy's early warning and detection systems {*yujing tance xitong*}, command and control [C2] {*zhihui kongzhi*} systems, communication hubs {*tongxin shuniu*}, and weapons control {*wuqi kongzhi*} systems; to conduct electronic deception {*dianzi qipian*} against the enemy, so as to conceal {*yinbi*} the operational intention {*zuozhan qitu*}; to execute jamming and suppression {*ganrao yazhi*} and destruction and sabotage {*cuihui pohuai*} of the enemy's important information system targets, to degrade the enemy's resistance capability; and to organize and implement information defense {*xinxi fangyu*}, to ensure friendly information system security and the bringing into play of these systems' effectiveness {*xiaoneng*}.

Section 1: Characteristics {*tedian*} of Joint Fire Strike Campaign IO…271

In a joint fire strike campaign, the battlespace {*zhanchang kongjian*} is expansive, the strike activities are diverse, and the information warfare [IW] {*xinxi duikang*} is unprecedentedly sharp. These cause IO to take on the following characteristics. **[end of page 271]**

I. Battlefield information awareness {*zhanchang xinxi ganzhi*} has become a prerequisite {*qianti*} and basis for campaign operations-research-based planning {*chouhua*}…272

Information is an important basis for various types of fire strike weapons system operations. Any type of long-range firepower system always includes an information assisting support {*xinxi zhiyuan*} content — target and missile positioning {*mubiao, daodan dingwei*}, meteorology, geodesy {*cedi*}, C2, and damage effects evaluation {*huishang xiaoguo pinggu*} — and not one such system can do without the assisting support of information systems. The reliance of firepower operations on information is growing ever higher. Battlefield information awareness will penetrate the entire joint fire strike process — intelligence collection, enemy situation assessment {*diqing panduan*}, command decision-making {*zhihui juece*}, target indication {*mubiao zhishi*}, fire strike,

and effects evaluation — and become a prerequisite for conducting joint fire strike. Battlefield information awareness capability already has become the critical factor {*guanjian yinsu*} in gaining the initiative {*zhudongquan*} in firepower operations and in gaining favorable opportunities for combat {*zhanji*}. To this end, the scope of battlefield information awareness will form all-around coverage of the entire battlespace, and ensure that the entire battlefield posture {*taishi*} is transparent to our side. It will enable real-time surveillance {监视 *jianshi*} and grasping of the battlefield dynamic state, and will provide reliable support {*baozhang*} for conducting rapid response and precision strike {*jingque daji*}.[12] If battlefield information awareness capability is inadequate, it certainly will influence the timeliness of command decision-making, and reduce fire strike effectiveness.

II. Information attack [offensive] {*xinxi jingong*} has become the "heavy fist" of fire strike…272

The basic focus of attention {*zhuoyandian*} of joint fire strike is to attack and destroy {*poji*} the enemy's operational system of systems [SoS] {*zuozhan tixi*}, and by comprehensively applying {*zonghe yunyong*} multiple operational means, with a combination of soft and hard {*ruanying jiehe*}, to strike at the critical nodes {*guanjian jiedian*} in the enemy's operational SoS, strip away the enemy's information superiority {*xinxi youshi*}, degrade its integrated-whole operational effectiveness {*zhengti zuozhan xiaoneng*}, and disintegrate the enemy's will to [fight a] war {*zhanzheng yizhi*}. Since the degree of reliance of the operational SoS on networked {*wangluohua*} information systems is extremely high, by having deviated from the support {*zhichi*} of various networks, the operational SoS could fall into paralysis {*tanhuan*}, and operational effectiveness could be greatly reduced. "Network sabotage" operations {"破网" 作战 *"powang" zuozhan*} already have become the most important link {*huanjie*} in joint fire strike. Moreover, information attack, with its intrinsic strong point in "network sabotage," has become the "heavy fist" of SoS attack and destruction {*tixi poji*}. To this end, before fire assault {*huoli tuji*}, [we] should carry out a preliminary {*xianqi*} information attack, and put effort into jamming and suppressing the enemy's air defense and anti-missile {*fangkong fandao*} reconnaissance and early warning {*zhencha yujing*}, target guidance {*mubiao yindao*}, and C2 systems, and attacking and destroying the enemy's air defense and anti-missile system, to screen {*yanhu*} the penetration {*tufang*} by our missiles and aviation forces {*hangkongbing*}. [We should] fully bring into play information attack's comprehensive superiority {*zonghe youshi*} in terms of broad cover area {*fugai miankuan*}, strong penetrating power {*chuantouli*}, and fire strike's long range (of fire) {*shecheng*}, **[end of page 272]** high precision {*jingdu*}, and great might {*weili*} — to execute key point strikes against the critical nodes and trunk links {主干链

[12] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

路 *zhugan lianlu*} within the enemy architecture {*tixi jiegou*}, and destroy its nodes, disturb its flow paths {*liucheng*}, paralyze its systems, sabotage its SoS, and degrade its effectiveness.

III. Degree of difficulty of command and adjustment control {*zhihui yu tiaokong*} is increased…273.

Within joint fire strike operations, IO activities and various firepower system operational activities are interweavingly carried out, the battlefield situation changes rapidly, command warfare {*zhihui duikang*} is sharp, the battlefield information quantity {*xinxiliang*} is sharply higher, the requirements {*yaoqiu*} on the integrated-whole quality {*zhengtixing*} of operations are stringent, and the factors which operational decision-making must consider have unprecedentedly increased. In addition, since the command system's role {*zuoyong*} of "nerve center" {*"shenjing zhongshu"*} is clear, it thus has even greater strike value, and has become the strike target of first choice for the engaging sides {*jiaozhan shuangfang*}. The IO command institution {*zhihui jigou*} not only must at the right time command and adjust-coordinate {*xietiao*} the IO activities of all services and arms {*zhu junbingzhong*} within the complex and changeable battlefield information environment, but also must continuously fight {*douzheng*} to protect itself and the safety of the various types of campaign command institutions. Survival and stability are faced with serious threats, and this has thus greatly increased the degree of difficulty of command and adjustment control.

IV. Fire strike and information attack are reciprocal "multipliers" {*"beizengqi"*} of operational capability {*zuozhan nengli*}…273

Information attack and fire strike are the two main operational activities of a joint fire strike campaign; they have consistency {*xiangrongxing*} and an interdynamic quality {*hudongxing*}. Within the phase of seizing information dominance {*zhixinxiquan*}, while applying means such as electronic warfare [EW] {*dianzizhan*} and network warfare {*wangluozhan*} to carry out information attack, [we] must use firepower to destroy the enemy's important information system nodes, in order to achieve the goal {*mudi*} of seizing information dominance. Joint fire strike with firepower kill {*huoli shashang*} as primary has accommodated the multilevel {*duocengci*} IO content. For example, exploiting IO reconnaissance enables detecting high-value targets, and can support the use of firepower to execute real-time destruction of those targets and to boost the fire strike effects; and effective information protection measures can provide secure support for fire strike operations. The information superiority acquired via IO has optimized {*youhuale*} the control of operational material {*wuzhi*} and capability {*nengliang*}, and thus has given fire strike even more accuracy {*zhunquexing*}, time effectiveness quality {*shixiaoxing*}, and security {*anquanxing*}. It is a multiplier which boosts the joint fire strike effectiveness. **[end of page 273]**

Section 2: Requirements of Joint Fire Strike Campaign IO…274

IO serves as operational activities which penetrate the entire process of a joint fire strike campaign and which have a major influence on the campaign's progress {*jincheng*} and outcome {*jieju*}. Within the entire campaign process, they have an extremely important position {*diwei*} and role. In organizing and implementing joint fire strike campaign IO, [we] should lay stress on grasping the following four issues.

I. Accurately grasping the relationship between fire strike and IO, and conducting integrated-whole operations-research-based planning…274

Joint fire strike possesses an overall situation quality {*quanjuxing*} and strategic quality {*zhanluexing*}, and it is closely correlated {*jinmi guanlian*} to political, economic, and diplomatic activities. To this end, we must stand on the high ground of national strategy and the military strategic overall situation; according to the strategic intent {*zhanlue yitu*}, conduct integrated-whole operations-research-based planning and thorough planning {*jihua*} for IO activities; accurately grasp the inherent relationship of IO to fire strike; properly and ably process the relationship of the joint fire strike's overall situation to the IO part; see that the IO activities are closely adjusted-coordinated {*miqie xietiao*} with the fire strike activities, and organically combine [the two]; and [thus] fully bring into play the integrated-whole might {*zhengti weili*} of IO and fire strike. When organizing and implementing joint fire strike IO, [we] must ably grasp the mutual complementary {*xianghu peihe*} and effects-wise mutually exploitative {*xianghu liyong*} relationship of joint fire strike to IO activities; lay stress on IO in the important directions, critical time segments {*guanjian shijie*}, and main activities within the joint fire strike campaign; and employ active activities to assist-support {*zhiyuan*} and complement the joint fire strike operations.

II. Comprehensively applying C2 methods to implement flexible {*linghuo*} command and adjustment control…274

A high-efficiency, flexible IO command SoS {*zhihui tixi*} is the critical link {*guanjian huanjie*} bearing on whether the joint fire strike campaign IO activities can be effectively implemented, as well as on whether [we] can realize their consistent adjusting-coordination with other operational activities. [We] should — based on the joint fire strike campaign command SoS, and focusing on the characteristics of IO command and strength application and on the situation of the IO equipment levels [standards] {*zhuangbei shuiping*} and **[end of page 274]** IO strength task organization {*liliang biancheng*} — keep attention on the requirements for implementing unified command {*tongyi zhihui*} of the multidimensionally integrated {*duoyuan yiti*} IO strengths, and construct a joint fire strike campaign IO command SoS, so as to form composite strength {*heli*}. Within the campaign implementation process, [we] must comprehensively apply the methods of planned control {*jihua kongzhi*}, ad hoc control {*linji kongzhi*}, targeted control {*mubiao kongzhi*}, and time control, to ensure implementing stable and sustained C2 over IO. For major IO activities, [we] must put

into effect highly centralized and unified {*jizhong tongyi*} planned control. The specific {*juti*} IO activities of all operational groups {*zuozhan jituan*}, with the ad hoc adjustment control mode {*suiji tiaokong fangshi*} as primary, are flexibly commanded by all operational groups. [We] must, based on each operational time segment's needs {*xuqiu*} for IO, implement flexible command and adjustment control, to ensure that the IO targets, activities, attack modes {*gongji fangshi*}, and attack key points are closely complemented by and mutually adjusted-coordinated with the mid- to long-range {*zhongyuancheng*} fire strike activities.

III. Focusing on weakening the enemy information system's integrated-whole operational capability, and precisely selecting the key point strike targets…275

Within joint fire strike, the prominent superiority of the adversary in terms of networked information systems and reconnaissance and early warning, C2, and rapid reaction will constitute a serious threat to our missile and aircraft penetration. This not only is where the main backing lies for the high-speed operation {*yunzhuan*} of the enemy's air defense and anti-missile SoS, but also is its distinct "soft rib." Hence, conducting suppression and destruction {*huishang*} of its critical information nodes, sabotaging its orderly operation {*youxu yunxing*}, and rendering it blind, uncontrollable, and unable to intercept {*xiangkan kanbujian, xiang kongzhi buliao, xiang lanlan buzhu*} [our missiles and aircraft] thus have become the most important missions of IO. Hence, [we] must firmly establish the consciousness of active attack [offensive] {*jiji jingong*}, comprehensively apply multiple information attack strengths, precisely select the key point strike IO targets, and use energetic and effective active attacks {*zhudong jingong*} and continuous attacks {*lianxu jingong*}. The key points are on conducting key point jamming and suppression and destruction and sabotage against the main targets within the enemy's reconnaissance and early warning, C2, and anti-missile and air defense information systems, such as ground-based satellite receiving stations, early warning aircraft, early warning radar stations {*yujing leida zhan*}, [Navy] observation and communication posts {*guantong zhan*}, C2 centers, communication hubs, microwave communication stations {*weibo tongxin zhan*}, and military satellite communication [facilities], as well as target indication radar {*mubiao zhishi leida*} and missile guidance radar {*daodan zhidao leida*} for air defense and anti-missile weaponry {*bingqi*}; to the maximum extent weakening and sabotaging **[end of page 275]** the operational effectiveness of the important electronic information systems which support {*zhicheng*} the enemy's integrated-whole defensive operations SoS {*zhengti fangwei zuozhan tixi*}; and thus weakening the enemy's integrated-whole defensive operational capability, so as to create favorable conditions for other operational activities.

IV. Centering on "being able to defend" {"防得住" *"fangdezhu"*}, and establishing a rigorous {*yanmi*} information defense system SoS…276

Within a joint fire strike campaign, maintaining the security of friendly information and information systems, and concealing our operational intention, are an important aspect in seizing information dominance. To this end, [we] must [implement]

strict electromagnetic [EM] spectrum management {*dianci pinpu guanli*}, to ensure the security of the campaign core information circulation {*xinxi liuzhuan*} process and of all types of electronic information systems and their critical nodes. In particular, [we] must strengthen information defense of important information system nodes, such as command communication hubs, weapons guidance and control systems, and the main-direction radar stations and observation and communication stations, and strengthen defensive measures in respects such as psychological protection and information secrecy {*baomi*} for the fire strike units, to ensure the smooth implementation of the joint fire assault activities. [We] must, on the basis of enhancing concealment and camouflage {*yinbi weizhuang*}, engineering protection, diversion and deception {*yangdong qipian*}, and EM [spectrum] management, exert effort to strengthen the building of an information defense SoS within the integrated air defense SoS {*zonghe fangkong tixi*}. [We must] emphasize using attack to aid defense {*yigong zhufang*}, and using active {*jiji*} information attack activities within air defense operations, to attack and destroy the enemy's air raid operations SoS {*kongxi zuozhan tixi*}; to weaken the enemy's two great superiorities , [viz.] "non-contact" and "high-precision" {*"feijiechu," "gaojingdu"*} [operations]; to gain the initiative in defense; and to ensure the battlefield survival and safety of our fire assault strengths, the normal operation of C2 systems, and the smooth implementation of the joint fire assault activities.

Section 3: Activities of Joint Fire Strike Campaign IO…276

IO activities within a joint fire strike campaign should be carried out by centering on the campaign phases of preliminary strike {*xianqi daji*}, sustained strike {*chixu daji*}, and follow-up strike {*houxu daji*}.

I. IO activities in the preliminary strike phase…276

Implementing IO in the preliminary strike phase mainly centers on the activities to seize local information dominance and air dominance/supremacy {*zhikongquan*} **[end of page 276]**. It should concentrate use of most of the information attack strengths within the task organization, to execute strikes against important information system targets, such as the enemy's command communication system, radar stations, and computer network nodes; spare no effort to seize local information dominance; and to the maximum extent degrade and even paralyze the operational effectiveness of the enemy information systems, so as to ensure the smooth conduct of our joint fire strike activities. The IO activities mainly are as follows: using information reconnaissance strengths to reconnoiter and evaluate-appraise the strike effects, so as to provide target information intelligence for sustained fire assault; using multiple information attack means such as electronic jammers {*dianzi ganraoji*}, long-distance assisting support jamming aircraft, and electronic jamming unmanned aerial vehicles [UAVs] {*wurenji*} to [conduct] key point jamming and sabotage of the air defense early warning and detection systems, C2 systems, communication networks, anti-missile interception systems, and airfield navigation systems within the enemy anti-missile SoS, so as to weaken the enemy's information acquisition, transmission, and processing capability and air-defense and anti-

missile operational capability; in the main assault direction, using anti-radiation weapons {*fanfushe wuqi*} and directed energy weapons [DEWs] {*dingxiang neng wuqi*} to attack the enemy airborne and sea-going reconnaissance and early warning platforms, so as to weaken the enemy's battlefield posture awareness capability and to assist-support and complement the fire strike activities of the missile, air, and naval operational groups; using network warfare strengths to execute attacks against the enemy computer network systems, so as to paralyze the enemy computer networks and sabotage the integrity {*wanzhengxing*} of the enemy operational SoS; and applying multiple information transmission media and psychological warfare [PSYWAR] {*xinlizhan*} weapons to execute psychological attacks against the enemy, so as to strengthen the shock effect of the missile strikes and boost the comprehensive benefit {*zonghe xiaoyi*} of the missile fire strikes.

II. IO activities in the sustained strike phase…277

In the sustained strike phase, the main mission for IO is to use the mode of accompanied assisting support {*bansui zhiyuan*} to maintain information superiority and to assist-support the firepower's sustained strike; at the same time it must have defense against attack {寓防于攻 *yufang yugong*}, and defend against the enemy's information attacks {*xinxi gongji*}. The main operational activities are as follows: the information reconnaissance strengths rigorously surveil the battlefield posture and enemy situation changes, constantly indicate targets for the fire strike strengths, and brief {*tongbao*} them on the situation and operational effects; the psychological operations [PSYOPS] {*xinli zuozhan*} strengths via various media execute high-intensity psychological attacks against the enemy, to enhance the shock quality {*zhenhanxing*} of the joint fire strikes; and the information deception strengths apply means such as information diversion {*xinxi yangdong*}, release of smoke screens, and spreading of metal chaff {*jinshu botiao*}, to screen the fire **[end of page 277]** strike strengths' assault on important targets in the enemy depth. At the same time, within the process of executing sustained fire strike, our information systems and facilities equipment {*shebei*} will be subject to the enemy's full-dimensional {*quanfangwei*}, multilevel, multi-means information attacks and firepower sabotage/destruction. In order to weaken to the maximum extent the enemy attack effects, [we] should adopt comprehensive measures, including EM emission {*dianci fushe*} control, information hiding {*xinxi yinni*}, electronic camouflage {*dianzi weizhuang*}, engineering protection, firepower screening, and using attack to aid defense, to strengthen information protection, and to defend against the ground, sea, air, and even outer space {*taikong*} information reconnaissance and information attacks executed against us by the enemy, to ensure the normal bringing into play of our information systems' effectiveness and the smooth conduct of the fire strikes.

III. IO activities in the follow-up strike phase…278

Implementing IO in the follow-up strike phase mainly centers on the campaign activities of supplementing {*buchong*} and expanding the fire strikes. On the basis of the previous phase's network sabotage and severing of links {破网断链 *powang duanlian*},

[our strengths will] conduct key point jamming and suppression and destruction and sabotage of the remaining and newly detected important information targets of the enemy, to maintain battlefield local information dominance, and to assist-support and complement the follow-up fire strike activities. Based on operational needs and requirements {*xuyao*}, [we will] at the right time apply network attack means to conduct infiltration {*shentou*} and sabotage of various types of network systems which maintain {*weixi*} war potential {*zhanzheng qianli*}. [We will] apply power grid {*dianwang*} attack weapons; watch the situation [for an opportunity] to sabotage the enemy's electric power system; and at the right time jam and sabotage the enemy's civilian radio {*guangbo*}, television, and telecommunications systems, to weaken the enemy's capability for assisting support to sustained operations {*zhiyuan chixu zuozhan de nengli*}. **[end of page 278; end of chapter]**

Chapter 16
Island Blockade Campaign {*daoyu fengsuo zhanyi*} Information Operations…279

An island blockade campaign is an offensive campaign {*jingong zhanyi*} which implements sea and air blockades against enemy-held islands {*dizhan daoyu*}. Its goals {*mudi*} are to sever the economic and military contacts between the enemy-held islands and the outside, and to weaken the enemy's operational capability {*zuozhan nengli*} and war potential {*zhanzheng qianli*}. The main missions of island blockade campaign information operations [IO] are as follows: to organize and implement IO reconnaissance {*zhencha*}, with the key points on ascertaining the situation of the composition, deployment {*peizhi*}, and technical parameters {*canshu*} of the enemy's counter-blockade operational reconnaissance and early warning systems {*zuozhan zhencha yujing xitong*}, command communication {*zhihui tongxin*} systems, and weapons control {*wuqi kongzhi*} systems; to widely carry out information fabrication {信息造势 *xinxi zaoshi*}, so as to deceive {*qipian*} and awe the enemy; to jam and suppress {*ganrao yazhi*} and destroy or sabotage {*cuihui pohuai*} the important information system targets {*mubiao*} of the enemy's counter-blockade operations, so as to weaken the enemy counter-blockade operational effectiveness {*zuozhan xiaoneng*}; to do all one can to sever the information contacts between the enemy-held islands and the outside, achieve a blockade of the enemy information field {*lingyu*}, and assist-support and complement {*zhiyuan, peihe*} the other blockade operational activities {*zuozhan xingdong*}; and to organize and implement information defense {*xinxi fangyu*}, to ensure our operational information security [INFOSEC] {*xinxi anquan*} and normally bring into play the effectiveness of [our] information systems.

Section 1: Characteristics {*tedian*} of Island Blockade Campaign IO…279

In an island blockade campaign, IO penetrates from the start to the finish of the operations, [involves] sharp confrontation {*duikang*}, and has taken on the following main characteristics. **[end of page 279]**

I. The operational activities' sensitiveness {*minganxing*} is strong, and the restricting factors {*shouzhi yinsu*} on IO activities are many…280

An island blockade campaign is an all-new campaign pattern {*zhanyi yangshi*} of local war under informationized conditions {*xinxihua tiaojianxia jubu zhanzheng*}. Its blockade space is a 3-dimensional [3-D] space {*liti kongjian*} including the water's surface, underwater [zones], and the air. The blockade areas (zones) {*fengsuo quyu*}, although offshore {*jinhai*}, nonetheless at the same time are also important international channels {*hangdao*} and vital communication [i.e., traffic] hubs {*jiaotong yaochong*}. Its main battlefield will be the vast international waters {*gonghai*} and international air zones {*kongyu*}, and often may involve other nations' political and economic interests. Within such a confused and complicated battlefield environment, operational activities

unavoidably will be subject to the restrictions of international laws and regulations {*fagui*}, and subject to political and diplomatic constraints and influence. If they are handled improperly {失当 *shidang*}, this could cause us in political terms and diplomatic terms to fall into a passive situation, and even to lose an opportunity for combat {*zhanji*}, or lead to a war's escalation {*zhanzheng shengji*}, and directly influence the campaign effects. Hence, IO must be rigorously {*yanmi*} organized and implemented based on political and economic needs and requirements {*xuyao*} and those of the joint campaign's overall situation {*quanju*}.

II. The campaign duration {*chixu shijian*} is long, and the missions for seizing information dominance {*zhixinxiquan*} are arduous…280

In an island blockade campaign, the aim lies in depleting the enemy's potential, until [we] wear down {*tuokua*} the enemy, and force the enemy to submit. If the adversary already has fully made material preparations {*wuzhi zhunbei*}, thought preparations, and operational preparations, we will find it very difficult to rapidly achieve the blockade goals, and this will often require a fairly long duration in order to gain a successful result. Within fairly long-duration island blockade operations, the operational opponent inevitably may fully exploit his reconnaissance and surveillance [R&S] {*zhencha jianshi*} system of systems [SoS] {*tixi*} and IO SoS, and, while devoting all effort to contending for {*zhengduo*} air dominance/supremacy {*zhikongquan*} and sea dominance {*zhihaiquan*}, will seize and maintain information dominance. Whether [one side] can effectively seize and maintain information dominance already has become the critical link {*guanjian huanjie*} in blockade operations. From the viewpoint of our military's present and future possibly developed IO, it is still difficult to achieve all-around information superiority {*xinxi youshi*}, and the missions for seizing information dominance will be extremely arduous. [We] must establish an underwater, surface, air, and information blockade SoS {*fengsuo tixi*}, and using high-maneuverability {*jidong nengli qiang*} platforms as primary, conduct active information attacks {*jijide xinxi jingong*} in the vast blockade operational areas (zones) {*zuozhan quyu*} and in different blockade operational directions. **[end of page 280]**

III. Blockade operational areas (zones) are vast, and the role {*zuoyong*} of air maneuver {*kongzhong jidong*} IO strengths is prominent…281

In an island blockade campaign, the sea battlefield is extremely vast. Due to the application of ocean R&S systems, long-range precision guided munitions [PGMs] {*yuancheng jingque zhidao wuqi*} systems, and battlefield information systems, the 3-D quality {*litixing*} and deepness {*zongshenxing*} of blockade operations have been further enhanced, and the tangible operational space {*zuozhan kongjian*} has acquired maximum expansion. Electronic warfare [EW] {*dianzizhan*}, network warfare {*wangluozhan*}, and psychological warfare [PSYWAR] {*xinlizhan*} moreover extend the blockade operational space into intangible electromagnetic [EM] {*dianci*}, network, and psychological space, so the operational space assumes multidimensional 3-dimensionality {*duowei liti*}. In conducting IO on such a multidimensionally integrated {*duowei yitihua*} battlefield, the

maneuver scope of ground EW strengths {*dianzi duikang liliang*} is restricted, and the operating distance {*zuoyong juli*} of shipborne EW strengths is limited. Only by having air maneuver IO force-strengths {*bingli*} with a large strike scope and high operational effectiveness executing active information attacks can [we] seize and maintain information dominance.

IV. Information blockade already has become a new means in island blockade operations…281

Information blockade signifies the use of various effective means to jam or sabotage the enemy's information infrastructure {*xinxi jichu sheshi*} and critical information system nodes {*jiedian*}, to block the acquisition {*huoqu*}, exploitation, and transmission of enemy information, and to halt the enemy information's effective flow, in order to create the conditions for gaining victory in the campaign. The goal of an island blockade campaign not only must be to cut off the enemy's economic contacts with the outside, but even more will require cutting off the enemy's information contacts with the outside. To this end, the blockading side can use an information blockade to cut off the enemy side's internal and external {*neibu yu waibu*} information connections and those internally among all operational units {*zuozhan danwei*}, so that the enemy cannot normally acquire and transmit necessary information, and to cause command paralysis {*zhihui tanhuan*}, force-strength activities going out of control {失控 *shikong*}, and economic, financial, and social chaos, thus weakening and even disintegrating the enemy's integrated-whole counter-blockade operational capability {*zhengti fanfengsuo zuozhan nengli*}. At the same time, it creates favorable conditions for the use of other blockade means, and achieves effects similar to those of a sea/air blockade. Hence, information blockade using EW and network operations as pillars already has become a new means in an island blockade campaign, and is the best policy {*shangce*}, superior to means such as obstacle blockade, firepower blockade, and force-strength blockade. **[end of page 281]**

Section 2: Requirements {*yaoqiu*} for Island Blockade Campaign IO…282

Island blockade campaign IO not only is an integrated-whole contention {*zhengti kangheng*} between the enemy and friendly sides {*diwo shuangfang*} in terms of science and technology [S&T] development levels {*fazhan shuiping*} and military information equipment {*xinxi zhuangbei*}, but also is a trial of strength in terms of wisdom and stratagem {智与谋 *zhi yu mou*}. The organizing and implementing of island blockade campaign IO should emphasize grasping the following four issues.

I. Based on the blockade campaign intention {*qitu*}, rationally determining the IO missions…282

Within an island blockade campaign, the opposing sides {*didui shuangfang*} will unfold {*zhankai*} sharp information warfare [IW] {*xinxi duikang*} in the land, sea, air, and space {*lu, hai, kong, tian*} battlefield; the battlespace {*zhanchang kongjian*} will be

expansive, the geographic environment will be complex, and the use of IO equipment will be restricted, so seizing battlefield information dominance will have a very high degree of difficulty. The IO missions should be rationally determined, based on the island blockade campaign intention. Usually, the main missions of island blockade campaign IO will be as follows: to jam the vital site electronic targets {*yaohai dianzi mubiao*} of the enemy's sea and air force-strengths, so as to assist-support all operational groups (groupings) {*zuozhan jituan (qun)*} in seizing local air dominance/supremacy and sea dominance; to jam and suppress the blockaded enemy's outside signal communication {*duiwai tongxin lianluo*}, and use the information blockade to assist-support all operational groups (groupings) in effecting 3-D blockade; to jam and suppress the electronic systems of key point military targets such as enemy harbors and airfields, so as to paralyze their command and control [C2] {*zhihui kongzhi*}, and assist-support all operational groups (groupings) at a favorable time opportunity {时机 *shiji*} in inflicting annihilative strikes {*jianmiexing daji*} on the enemy; and to jam and suppress the electronic targets of a preempting or counter-preempting {*xianzhi huo fanzhi*} enemy, so as to assist-support all operational groups (groupings) in thwarting the enemy intention to sabotage the blockade.

II. [Implementing] unified command {*tongyi zhihui*}, and closely adjusting-coordinating {*miqie xietiao*} the IO activities…282

In an island blockade campaign, the campaign strengths are multidimensional {*duoyuan*}, the information essential factors {*xinxi yaosu*} are many, and the operational activities are diverse. [The joint campaign commander (JCC)] must set out from the overall situation of the campaign {*zhanyi quanju*}, put into effect unified command of the professional {*zhuanye*} IO strengths and various nonprofessional IO strengths in all services and arms {*junbingzhong*} participating in the campaign, rationally disposition {*bushu*} them, and form an integrated-whole composite strength {*zhengti heli*} for IO against the enemy. He must establish a unified IO **[end of page 282]** command and adjusting-coordination institution {*zhihui xietiao jigou*}, for unified planning and organizing {*tongyi jihua zuzhi*} of the activities of all services' and arms' IO strengths; he must, based on the general plan {*zongti jihua*} for the island blockade campaign, focus on the overall situation, and center on the campaign's main operational activities, to formulate an IO activities plan; and he must organically combine the IO activities of all services and arms and of all campaign directions {*zhanyi fangxiang*}, all campaign phases, and the front and rear {*qianhou*}, to realize interaction {*xianghu zuoyong*} of IO effects. In the use of operational strengths, he must area (zone) by area (zone) and mission by mission {*fen quyu, an renwu*} carry out combined organizational grouping {*hecheng bianzu*} of the IO units (elements) {*bu (fen) dui*} of all services and arms. In terms of the operational SoS {*zuozhan tixi*}, he must tightly combine {*jinmi jiehe*} the activities at sea and in the air, on the surface and underwater, and at the front and rear, to constitute a full-dimensional {*quanfangwei*}, full-frequency-domain {*quanpinyu*}, large-depth, 3-D IO system. Via thorough planning and adjusting control {*tiaozheng kongzhi*}, [he should] see that the land, sea, air, space, and EM operational activities, according to mission, time, and area (zone), constitute a mutually assisting-supporting, mutually

complementary integrated-whole SoS, which to the maximum degree will bring into play an integrated-whole superiority.

III. Synthetically applying {*zonghe yunyong*} multiple means in key point blockade operational areas (zones) to achieve local information blockade…283

Once the island is totally blockaded, its economy inevitably will be paralyzed, and this will set off social unrest and create instability in the political situation. Hence, the adversary inevitably may devote all effort to striking at and destroying our blockade force-strengths and weapons {*bingli, bingqi*}, maintaining {*weihu*} the safety of the navigation routes to the outside {*duiwai hangxian*}, and watching for a chance to penetrate the blockade. To this end, the island blockade campaign must tightly center on the overall situation of the blockade campaign, and synthetically apply IO means such as electronic attack {*dianzi gongji*}, computer network infiltration {*jisuanji wangluo shentou*}, psychological attack {*xinli gongji*}, and force-strength and firepower strike, to form an information attack momentum {势 *shi*} with a mutual combination of EM space, network space, and the psychological field {*xinli lingyu*}, and with a mutual combination of ground, sea surface, and air, so as to seize local information dominance and to support the operational activities of the main blockade force-strengths.[13] The island blockade campaign in terms of spatial scope has many points, broad areas, and long lines; our IO strengths are limited, and can only support the operational activities in the main blockade operational areas (zones). [The JCC] must, based on the blockade operational direction and operational time and on the needs and requirements of the operational activities, accurately grasp the key points of the campaign blockade areas (zones), blockade targets, blockade time opportunities, and blockade strengths; concentrate use of {*jizhong shiyong*} the IO strengths; use active {*jiji*} **[end of page 283]** IO activities; and [thus] achieve local information blockade in the key point blockade operational areas (zones).

IV. Relying on the abundant superiority in information resources, to ensure the information blockade's capability for sustained operations {*xuzhan nengli*}…284

Within the island blockade campaign, [the JCC] can fully exploit the many superiorities of the coastal areas' {*yanhai diqu*} developed civilian information networks and abundant information resources for communications, traffic, banking/finance, and electric power, and in terms of IO equipment and instrument equipment {*zhuangbei qicai*} quantities and classes {*zhonglei*}, to maintain the information blockade's capability for sustained combat. To this end, he must — under the unified command of the island blockade campaign command institution, and based on the natural geographic situation of the blockade operational areas (zones), the changing situation of the air

[13] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

battlefield, and the characteristics of the military/civilian-service {*jundi*} IO strengths — differentiate the missions {*qufen renwu*}; closely coordinate {*miqie xietong*}; and form an IW posture {*xinxi duikang taishi*} which has soldiers working as civilians {寓兵于民 *yubing yumin*}, the whole people participating in combat {*quanmin canzhan*}, and integrated-whole confrontation {*zhengti duikang*}. [He should] mobilize {*dongyuan*} and rely on the masses of people, adopt multiple military-civilian general purpose IO fighting methods {*zhanfa*} which are simple and easily implemented, and rely on powerful theater {*zhanqu*} information resources — to maintain uninterrupted {*bujianduan*} strength replenishment {*liliang buchong*}, to provide full IO support, and to ensure the IO's powerful offensive {*gongshi*} and capability for protracted {*chijiu*} sustained operations.

Section 3: Island Blockade Campaign IO Activities…284

Island blockade campaigns usually are partitioned {*huafen*} into a blockade force-strength unfolding phase, a phase for seizing blockade operations-area dominance {*kongzhiquan*}, a sustained blockade {*chixu fengsuo*} phase, and a phase for concluding the campaign. In organizing and implementing island blockade campaign IO, [the JCC] should focus on the needs and requirements of the strategic overall situation {*zhanlue quanju*}; meticulously perform operations-research-based planning {*chouhua*} and organizing; concentrate elite {*jingrui*} IO strengths in the main blockade direction, important sea and air blockade operational areas (zones), and critical time segments {*guanjian shijie*}; and closely coordinate with the sea and air operational groups, to assist-support and complement the island blockade activities.

I. IO activities in the blockade force-strength unfolding phase…284

The JCC {*lianhe zhanyi zhihuiyuan*} and his command organ {*zhihui jiguan*} should, based on the island blockade campaign intention **[end of page 284]** and the IO plan, uninterruptedly collect [data on] the situation of the enemy's counter-blockade operational preparations; strictly control EM radiation {*dianci fushe*}, and when necessary implement radio silence {*wuxiandian jingmo*}; in good time organize sea, air, and ground electronic diversion/demonstration {*dianzi yangdong*} and information deception {*xinxi qipian*}, combine it with force-strength diversion, and implement information fabrication; adopt multiple means to jam and suppress the enemy's R&S and early warning and detection systems, to screen the blockade force-strengths' maneuver and unfolding; and employ sea and air IO strengths to screen submarines {*qianting*} and aviation forces {*hangkongbing*} in conducting mine-laying, and complement all services and arms in establishing a reconnaissance patrol distribution system {*zhencha xunluo peixi*}, underwater obstacle blockade distribution system {*shuizhong zhang'ai fengsuo peixi*}, air blockade and sea maneuver and strike distribution system {*kongzhong fengsuo he haishang jidong daji peixi*}, and fire strike distribution system, to form a blockade posture.

[They should] adopt various modes to conduct public opinion deception {*yulun qipian*} against the enemy, to paralyze and confuse the enemy, and to give the enemy

difficulty in ascertaining our timing {*shiji*} and modes for implementing blockades. At the same time, [they should] in China's interior conduct education in implementing blockades of enemy-held islands, and effectively be on guard against the enemy military's psychological offensives {*xinli jingong*}, to make the numerous officers and men fully recognize the significance of the blockade operations, to boost our military's troop morale {*junxin shiqi*}, and to preserve the high stability and cohesive force {*ningjuli*} of units participating in the blockade operations.

[They must] set up network firewalls {*wangluo fanghuoqiang*}, to guard against computer viruses {*jisuanji bingdu*} invading out operational networks, as well as to defend against enemy computer "hacker" {*"heike"*} infiltration; to protect the security of our operational networks and of their internal resources; and to ensure during campaign unfolding the normal operation {*yunzhuan*} of all operational networks. They must adopt various measures for concealment {*yinbi*}, camouflage {*weizhuang*}, deception, and decentralized deployment {*fensan peizhi*}, to guard against the enemy, within the counter-preemption operations it can conduct, effecting destruction of network systems in our blockade operations.

The operational groups of all participating services and arms must adopt various measures to carry out rigorous camouflage, and do a good job of concealment; and they must implement an information blockade. When necessary they can expel correspondents from hostile nations, to guard against too early disclosure of our blockade intention. Once the blockade operations are declared, all blockade operational groups must in swift and concealed fashion maneuver to the predetermined operational areas (zones), progressively unfold in the blockade operations' sea areas {*haiqu*} and air zones, and form a 3-D blockade SoS, to shorten the enemy's time for the acquisition and exploitation of information on our implementation of the blockade. **[end of page 285]**

II. IO activities in the phase of seizing blockade operational-area dominance…286

The JCC and his command organ should rigorously organize the IO activities within seizing information dominance, air dominance/supremacy, and sea dominance, and within resisting the enemy's counter-preemption, so as to create favorable conditions for seizing blockade operational-area dominance.

Seizing information dominance is the core of seizing the initiative {*zhudongquan*} in blockade operations. They should establish a land, sea, air, and space integrated {*yiti*} IO reconnaissance distribution system, to rigorously surveil and accurately grasp the situation of the enemy's IO force-strengths and weapons and its EM activity {*huodong*}, so as to provide a foundation for IO command decision-making {*zhihui juece*} and operational activities. They should concentrate use of the campaign's directly subordinate electronic offensive [attack] {*dianzi jingong*} strengths as well as those of the various services and arms, and under coordination with and complementation by other operational strengths, conduct key point jamming and suppression and destruction or sabotage of the vital site targets in the enemy's counter-blockade

operational information system. [They should] at the right time apply network attack strengths to execute attacks on the network systems of the enemy's operational SoS, and to seize battlefield local information dominance, so as to create favorable conditions for the blockade operational activities.

When seizing air dominance/supremacy, they should take the air information attack strengths as primary, and synthetically apply multiple information attack strengths, for key point jamming and suppressing and destroying or sabotaging of enemy early warning and detection systems, air defense and anti-missile command communication {*fangkong fandao zhihui tongxin*} systems, air defense weapons control systems, and information attack {*xinxi gongji*} systems which constitute threats to our air blockade operational activities, so as to assist-support and complement our operational activities to seize air dominance/supremacy.

When seizing sea dominance, they should synthetically apply multiple information attack means, by air, sea, and land, for key point jamming, destruction, or sabotage of the enemy surface warning and detection {*duihai jingjie tance*} systems, command communication systems, air defense weapons control systems, and information attack systems which constitute threats to our sea blockade operations, so as to assist-support and complement our operational activities to seize sea dominance.

When resisting the enemy's counter-preemption, they should in unified [fashion] organize and command all IO groups (groupings) to actively complement the other operational strengths' resistance operational activities. [They should] synthetically apply information attack strengths, for key point jamming, destruction, or sabotage of the enemy's command communication systems, weapons control systems, and information attack systems, so as to degrade the enemy counter-preemption operational capability. For important targets, [they should] adopt **[end of page 286]** means such as electronic protection and concealment and camouflage, and coordinate with other operational strengths to safeguard {*baowei*} the security of the important targets. In the phase for seizing blockade operational-area dominance, they should fully exploit means such as various types of propaganda and PSYWAR weapons, to execute psychological attacks against the enemy, so as to complement the operational activities of the other information attack strengths; and for important information targets, [they should] adopt information defense measures, to ensure our operational INFOSEC and the bringing into play of the information systems' effectiveness.

III. IO activities in the sustained blockade phase…287

The JCC and his command organ should base themselves on protracted operations {*chijiu zuozhan*}, and uninterruptedly organize and command the IO strengths, while conducting continuous R&S of the enemy's important information system targets, in concentrating use of information attack strengths to conduct jamming and suppression and destruction or sabotage against those targets, so as to assist-support and complement the sustained blockade by the Navy, Air Force, and Second Artillery Corps against the

enemy's air and sea lines of communication [SLOC] {*haishang jiaotongxian*}, and their sustained sabotage activities against important targets in the enemy-held islands.

During sustained blockade of SLOC, [the JCC and command organ] should carry out rigorous monitoring {监控 *jiankong*} of EM signals and hydroacoustic signals {*shuisheng xinhao*} in the important blockade operational areas, to timely grasp the dynamic state {*dongtai*} of the enemy penetration force-strengths {*tupo bingli*} and anti-submarine force-strengths {*fanqian bingli*}. For newly detected enemy concealed electronic information targets and mobile detection and early warning {*jidong tance yujing*} systems, [they should] carry out reconnaissance and positioning {*dingwei*}, and conduct jamming and suppression or destruction and sabotage of them. [They should] strengthen surface R&S {*haimian zhencha, jianshi*} of the blockade mine area {*leiqu*} situation, to provide intelligence assisting support {*qingbao zhiyuan*} for timely organizing of activities such as follow-up mine laying {*houxu bulei*} and submarine ambush and roving/hunting {*qianting shefu, youlie*}. [They should] organize IO reconnaissance strengths to complement the other reconnaissance strengths in carrying out detection and positioning of commercial ships and transports {*yunshu jianchuan*} which violate restricted navigation areas {*jinhangqu*}, and swiftly ascertaining their nature, to provide target information for the blockade force-strengths implementing of interception, visiting and inspection {临检 *linjian*}, and seizure {*nabu*}, and to assist-support and complement the naval operations {*haishang zuozhan*} strengths in driving away {驱离 *quli*}, intercepting, and striking at transports which enter the restricted navigation areas.

During sustained blockade of air lines of communication {*kongzhong jiaotongxian*}, [the JCC and command organ] should organize IO reconnaissance strengths to complement the other reconnaissance strengths in timely ascertaining the attributes {*shuxing*} and quantity of aerial vehicles {*hangkongqi*} entering our no-fly areas {*jinfeiqu*} and their adjacent air zones, to provide target intelligence for the aviation forces and surface-to-air missile [SAM] units {*dikong daodan budui*}; **[end of page 287]** and [they should] organize information attack strengths to conduct jamming and suppression of the information systems of enemy-nature {敌性 *dixing*} aerial vehicles entering the no-fly areas, so as to assist-support and complement our aviation forces and SAM units in driving them away, forcing their landing, and intercepting and striking at them.

When conducting sustained sabotage of important targets on the enemy-held islands, [the JCC and command organ] should organize information attack strengths in jamming, destroying, or sabotaging the enemy's important information system targets, to assist-support the strike activities of the Second Artillery Corps and of the naval and Air Force aviation forces {*hai, kongjun hangkongbing*}. In the sustained blockade phase, [the JCC and command organ] also should, based on operational needs and requirements, apply network attack means to execute attacks against the network systems of the enemy's counter-blockade operational SoS; uninterruptedly exploit various types of public opinion propaganda means and PSYWAR weapons to execute psychological

attacks against the enemy, demonstrate our military's operational will and resolve, and induce anti-war [sentiment] and war-weariness {*fanzhan he yanzhan qingxu*} in the enemy military and civilians; and thoroughly organize information defense activities with our important information system targets as the key points.

IV. IO activities in the phase of concluding the campaign…288

When concluding the campaign in a blockade campaign, the JCC and his command organ should continue to thoroughly organize IO activities, to timely provide assisting support for our blockade force-strengths in safe withdrawal from the blockade sea and air zones or when shifting into a new campaign pattern.

When the blockade force-strengths withdraw from the battlefield, [the JCC and command organ] should organize IO reconnaissance to complement the other reconnaissance strengths in rigorous surveillance of the movements {*dongxiang*} of enemy ships and aircraft, to guard against enemy surprise raids {*turan xiji*}, and organize information attack strengths for key point jamming and suppression of enemy airborne and shipborne radar and command guidance communication {*zhihui yindao tongxin*}, so as to screen the blockade force-strengths in safely and swiftly withdrawing from the blockade operational area. When necessary, [they must] synthetically apply multiple means to create the false impression {假象 *jiaxiang*} that our blockade force-strengths are continuing to be present in the blockade sea and air zones, so as to deceive and confuse the enemy. At the same time, [they should] strengthen examination of the news [media] {*xinwen shencha*}, and strictly control the scope and mode of broadcasts of operational information, to ensure the security and secrecy {*anquan baomi*} of the operational information. When preparing to shift into another campaign pattern, they should swiftly readjust the missions and disposition {*tiaozheng… renwu he bushu*} of the IO strengths, and do a good job of the next phase's IO preparations, to create the conditions for accomplishing the new campaign missions. **[end of page 288; end of chapter]**

Chapter 17
Island Offensive Campaign {*daoyu jingong zhanyi*} Information Operations…289

An island offensive campaign is a sea crossing {*duhai*} offensive campaign conducted against an enemy entrenched on islands. Within an island offensive campaign, in order to maintain the campaign initiative {*zhudong*}, the engaging sides {*jiaozhan shuangfang*} will widely apply information operations [IO] means to first seize information dominance {*zhixinxiquan*}. Island offensive operations under informationized conditions {*xinxihua tiaojianxia*} will be carried out within a complex electromagnetic [EM] environment {*dianci huanjing*}; IO will infiltrate into every field {*lingyu*} and every direction of the campaign, and not only will be the guide {先导 *xiandao*} for the campaign, but also will penetrate from the beginning to the end of the campaign. Seizing information dominance will have important significance for seizing and maintaining air dominance/supremacy {*zhikongquan*} and sea dominance {*zhihaiquan*} in the island offensive campaign, and even for seizing the initiative {*zhudongquan*} and ultimate victory in the entire campaign.

The main missions of island offensive campaign IO are as follows: to organize and implement IO reconnaissance {*zhencha*}, with the key points on ascertaining the situation of the composition, deployment {*peizhi*}, and technical parameters {*canshu*} of the enemy's reconnaissance and early warning systems {*zhencha yujing xitong*}, command and control [C2] {*zhihui kongzhi*} systems, communication hubs {*tongxin shuniu*}, and weapons control {*wuqi kongzhi*} systems in the main operational direction {*zhuyao zuozhan fangxiang*} and important zones (sea zones) {*di (hai) yu*}; to jam and suppress {*ganrao yazhi*} the information system critical nodes {*guanjian jiedian*} and important targets of the enemy's C2 centers, communication hubs, and radar [sets]; and to resist and defend against {*kangyu*} the enemy's outer space {*taikong*}, air, ground, and sea information attacks {*xinxi gongji*}, so as to ensure our operational information security [INFOSEC] {*xinxi anquan*} and the normally brought into play effectiveness {*xiaoneng*} of the information systems. **[end of page 289]**

Section 1: Characteristics {*tedian*} of Island Offensive Campaign IO…290

An island offensive campaign is a strategic-quality campaign {*zhanluexing zhanyi*} conducted under specific {*teding*} conditions. Its scale is huge, its goals {*mudi*} are firm, its operational background is complex, and its operational activities {*zuozhan xingdong*} will unfold {*zhankai*} in the land, sea, air, space, and EM {*lu, hai, kong, tian, dian*} multidimensional space {*duowei kongjian*}. IO will penetrate the entire process [of the campaign], and will have the following main characteristics.

I. IO is the prerequisite {*qianti*} and basis for seizing sea dominance and air dominance/supremacy, and will become the leading activity of the island offensive campaign…290

Within island offensive campaign operations, seizing information dominance has decisive significance for seizing air dominance/supremacy and sea dominance. IO will be the opening prelude to the island offensive campaign, and as the campaign's guide it will bring into play an important role {*zuoyong*} at the start of the campaign's launch. IO also is a prerequisite and basis for seizing sea dominance and air dominance/supremacy within the island offensive campaign. Seizing air dominance/supremacy first of all relies on information dominance. The struggle {*douzheng*} in the contention {*zhengduo*} for air dominance/supremacy inevitably will unfold by centering on seizing information dominance, and losing information dominance certainly will mean losing air dominance/supremacy. Seizing sea dominance also relies on information dominance. Within the development process for modern warships {*junjian*}, various types of information systems, especially communication facilities equipment {*tongxin shebei*} and target detection {*mubiao tance*} gear, are growing day by day and becoming increasingly complex; they have become important components {*zucheng bufen*} of weapons systems. In order to enhance defense capability {*fangyu nengli*}, a good many ships also have been outfitted with electronic jamming equipment {*dianzi ganrao zhuangbei*}, so that the contention for sea dominance and air dominance/supremacy will be fully embodied in the comprehensive confrontation {*zonghe duikang*} of information systems. One can foresee that in an island offensive campaign, the contention in the information field will be ever sharper, IO will be fused into an organic whole {*yiti*} with seizure of air dominance/supremacy and sea dominance, and operational activities will from start to finish center on the sharp confrontation for seizing and maintaining information dominance. **[end of page 290]**

II. Participating strengths {*canzhan liliang*} are numerous, and the IO system confrontation {*xitong duikang*} feature {*tezheng*} is distinct…291

An island offensive campaign is a typical omni-service and arm {*zhu junbingzhong*} joint campaign. The opposing sides {*didui shuangfang*} both will inject numerous campaign strengths within the operational area (zone) {*zuozhan quyu*}; the units of the various services and arms carrying out different missions will simultaneously unfold activities in the air, at sea (under water), and on land in specific areas (zones), and even in outer space {*waiceng kongjian*}; situations will be complex and changeable, and the war situation {*zhanju*} will assume a dynamic state mutually interweaving attack with defense and interior lines with external lines. Operational activities will unfold in the land, sea, air, space, and EM multidimensional space; IO will penetrate into every field, every direction, every phase, and every operational pattern {*zuozhan yangshi*} and all operational activities of the joint campaign; and IO systems will join the entire battlefield into an organic whole, to form an operational system of systems [SoS] {*zuozhan tixi*} with the strengths highly combined {*hecheng*}. The opposing sides, centering on the contention for battlefield local information superiority {*jubu xinxi youshi*}, will inject

numerous IO strengths, and at many levels {*cengci*}, land, sea, air, space, and EM, will unfold a series of information attack and defense activities {*xinxi gongfang xingdong*}. These IO strengths not only come from the professional IO units {*zhuanye xinxi zuozhan budui*} of all services and arms, but also originate from the nonprofessional IO units or departments of the armed forces and civilian sector {*jundui yu minjian*}, and sometimes also can draw upon international open source or secret {*mimi*} information channels. This has thus made the battlefield IO space assume trends of multidimensionalization {*duoweihua*}, globalization {*quanqiuhua*}, and integration {*ronghehua*}. The enemy and friendly sides' {*diwo shuangfang*} information warfare [IW] {*xinxi duikang*} in its essence is an integrated-whole confrontation of IO systems, and all services' IO strengths must divide their labor clearly and lay stress on key points {*zhongdian*}, in order to be able to bring into play integrated-whole operational effectiveness {*zhengti zuozhan xiaoneng*}. IO systems per se also have vulnerability {*cuiruoxing*}: when a break {*duanlian*} occurs in any one link {*huanjie*} of a system, it always could influence its integrated-whole function {*zhengti gongneng*}. All operational strengths also must closely coordinate {*miqie xietong*}, and be complete in both attack and defense {*gongfang xiangqi*}, in order to maintain the normal operation {*yunxing*} of the information systems.

III. The battlefield environment is complex, and IO support {*baozhang*} missions are arduous…291[14]

Island offensive campaign battlespace {*zhanchang kongjian*} EM signals will be numerous in quantity, high in density, and complex in system {*tizhi*} [i.e., format]. They will include not only communication signals and radar signals, but also the signals emitted by electro-optical [EO] facilities equipment {*guangdian shebei*} and hydroacoustic facilities equipment {*shuisheng shebei*} and by their radiation sources {*fusheyuan*}; they will include not only the signals of Navy and Air Force electronic facilities equipment {*dianzi shebei*}, but also the signals of Army {*lujun*} electronic facilities equipment; and they will include not only signals in conventional systems, but also **[end of page 291]** signals in new systems, and thus will make the battlefield EM environment extremely complex. In addition, the degree of system integration {*xitong jicheng*} in IO is high, its technical content is high, its performance is advanced, its classes {*zhonglei*} are numerous, its technical maintenance {*weihu*} is complex, and its requirements {*yaoqiu*} on technical support are very stringent. Added to this, overseas operations {*kuahai zuozhan*}, far from land bases {*luji*}, have an extremely pronounced contradiction {*maodun*} between damage {*sunhuai*} and support in situations where they

[14] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

encounter key point strikes; and this has levied new and even more stringent requirements on restoring "regeneration" {*"zaisheng"*} capability.

IV. The information infrastructure {*xinxi jichu sheshi*} is fairly weak, and restricts the bringing into play of the integrated-whole capability {*zhengti nengli*} of IO…292

Our military's battlefield information infrastructure construction got started fairly late. Communication means such as fiberoptic (electric) cables {*guang (dian) lan*}, satellites, and digital microwave {*shuzi weibo*} and shortwave radio sets {*duanbo wuxiandian tai*} still have not been formed into systems which are 3-dimensional [3-D] {*liti*}, can cover the entire operational space {*zuozhan kongjian*}, and integrate multiple functions {*zonghe duogongneng*}. In terms of command information systems, we still have not completely achieved integration {*yitihua*} of battlefield weapons systems and integration of information systems, and cannot completely accomplish tri-service intercommunication {*sanjun hutong*} and information sharing {*xinxi gongxiang*}; our information attack and information defense capabilities are still relatively weak; and seizing and maintaining information dominance will be subject to fairly high threats and restrictions. This has restricted the bringing into play of integrated-whole operational capability {*zhengti zuozhan nengli*}.

Section 2: Requirements for Island Offensive Campaign IO…292

Based on the characteristics of IO and on the reality of existing equipment {*zhuangbei*}, within island offensive campaign IO, [we] must tightly center on the campaign intention {*zhanyi qitu*}, concentrate on the main contradictions, and excel at working out an approach to [information] fabrication {谋划造势 *mouhua zaoshi*}, to fully bring into play the maximum effectiveness of all essential factors {*yaosu*} of IO, and to seize local information dominance.

I. Focusing on joint operations, and implementing unified command {*tongyi zhihui*}…292

In island offensive campaign IO, the participating strengths are multidimensional {*duoyuan*}, the means are diverse, and the distribution scope {*fenbu fanwei*} is broad. In particular, the operational groups {*zuozhan jituan*} and operational units {*zuozhan budui*} of all services and arms not only have relative independence, but also are an organically combined operational integrated whole {*zuozhan zhengti*}; and their campaign activities {*zhanyi xingdong*} are interconnected {*xianghu lianxi*}. **[end of page 292]**

They must overcome the traditional thought of ground operations {*dimian zuozhan*} and of a single service and arm; strengthen the concept {*guannian*} of joint operations; and via unified command, and unified operations-research-based planning {*tongyi chouhua*} of IO in the land, sea, air, space, and EM fields, synthetically apply {*zonghe yunyong*} soft, hard, attack, and defense {软, 硬, 攻, 防 *ruan, ying, gong, fang*}

means. This will enable consistent adjusting-coordination {*xietiao*} of IO strengths — in different directions, in different spaces, of different types {*leixing*}, and at different levels — to form an integrated-whole composite strength {*zhengti heli*}, and seize and maintain local information dominance. First is the need to implement a command mode {*zhihui fangshi*} with a combination of centralized and decentralized command {*tongfen jiehe*}. [The joint campaign commander (JCC)] must, based on the campaign needs and requirements {*xuyao*} and the battlefield's actual situation, flexibly {*linghuo*} adopt command modes which implement decentralized command {*fensan zhihui*} per level {*ancengci*} and implement centralized command {*jizhong zhihui*} per need {*anxu*}, to accomplish the combination of centralized and decentralized, centralized but not "rigid" {"死" *"si"*}, decentralized but not "disordered" {*"luan"*}, and boost command time effectiveness {时效 *shixiao*}. Second is the need to formulate a unified IO plan {*jihua*}. Setting out from the needs and requirements of integrated-whole operations and from the high ground of seizing information dominance, and based on the campaign's overall intention, he determines the IO targets, clarifies the missions, differentiates the strengths, and performs unified operations-research-based planning {*tongchou*} for using the various types of information resources, to ensure the consistent adjusting-coordination and operational effects of the campaign activities. Third is the need to unify the IO activities. Per the unified IO plan, he organizes the information strengths of all participating services and arms and all units, as well as the local area; implements unified information attack activities; and achieves IO activities which can be mutually assisting-supporting {*xianghu zhiyuan*} and closely complementary {*miqie peihe*} in different directions, different spaces, different categories {*leibie*}, and different levels, to bring into play to the maximum extent an integrated-whole superiority.

II. Grasping the operational centers of gravity [COGs] {作战重心 *zuozhan zhongxin*}, and forming local superiority…293

A joint campaign's operational COGs generally signify the critical link points [nodes] {*guanjie dian*} which can realize the strategic intent {*zhanlue yitu*} and the campaign objectives {*zhanyi mubiao*}, or the focal points which the enemy and friendly sides must contest and which can influence the overall situation of the campaign {*zhanyi quanju*}. The island offensive campaign battlefield is vast; under circumstances where our IO strengths have difficulty within a short time in all-around resistance to a powerful enemy, only by grasping the campaign's operational COGs, implementing local aggregated superiority {局部聚优 *jubu juyou*}, and using the limited IO strengths at the crucial points {到刀刃上 *dao daoren shang*}, can [we] ensure seizing local information dominance. First is the need to form superiority in the main direction. An island offensive campaign can simultaneously have several operational directions, and the status {*diwei*} occupied by each operational direction within the overall situation **[end of page 293]** is different. If one has fought well in the main direction, it could play a decisive role {*qi juedingxingde zuoyong*} in the entire war situation. [The JCC] must use the main IO strengths in the main operational direction influencing the overall situation, to form an overwhelming superiority, and support the progress {*jincheng*} and development of the main operational direction. Second is the need to form superiority in the main operational

activities. He must concentrate use {*jizhong shiyong*} of IO strengths in the critical operational time segments {*guanjian zuozhan shijie*} — seizing the "three dominances" {*"sanquan"*}, the navigational crossing transportation {*hangdu shusong*}, the 3-D penetration {*liti tupo*}, and resisting the enemy counterattack {*fanji*} — and in the main operational activities. Third is forming superiority at the key point targets {*zhongdian mubiao*}. He must determine these based on the joint campaign operations' intent and goals; synthetically apply various strengths and means to strike at the source, sever the critical links {*guanjie*}, and attack the vital sites {*yaohai*}; effect key point destruction of the enemy's forward bases {*qiangjin jidi*} and sea and air operational platforms; strike at the enemy airborne early warning {*kongzhong yujing*} systems and sea and air command platforms; paralyze {*tanhuan*} the enemy's communication, radar, computer network, and command automation {*zhihui zidonghua*} systems; destroy the enemy IO systems' main battle equipment {*zhuzhan zhuangbei*} and critical positions {*guanjian buwei*}; cause enemy network paralysis, information interrupts {信息中端 *xinxi zhongduan*}, command dysfunction {指挥失灵 *zhihui shiling*}, weaponry going out of control {兵器失控 *bingqi shikong*}; and to the maximum degree weaken and reduce or stop {减煞 *jiansha*} the attack superiority of the enemy's high-tech weaponry. Fourth is synthetically applying the multiple IO means and methods of all services and arms. He must center on the operational missions; correctly determine the operational steps and the employment sequence {*shiyong shunxu*} for the strengths; unify the planning for using the various IO resources; and synthetically apply all services' and arms' multiple IO means and methods, in each battlefield, each field, and all phases of the campaign, to execute full-depth {*quanzongshen*}, multi-field continuous strikes against the enemy. He must concentrate on the critical time domain {*shiyu*}, space domain {*kongyu*}, and frequency domain {*pinyu*}; grasp the key points for use of troops; concentrate the injection of superior force-strengths to execute key point strikes at the enemy's vital site targets {*yaohai mubiao*}; and strive to fight no battle unless painful blows, paralysis, and destruction are certain {不打则已, 打则必痛, 必瘫, 必毁 *buda zeyi, daze bitong, bitan, bihui*}.

III. Keeping a foothold in preempting the enemy {*xianji zhidi*}, and persisting in active attack {*jiji jingong*}…294

Active attack has reflected the general laws {*guilyu*} of operations under informationized conditions, and is a special {*teshu*} requirement for struggle in the information field. Island offensive campaign IO is different from past operations' fighting methods {*zhanfa*} of "avoiding the enemy's spearhead, and awaiting an opportunity to defeat the enemy" {"避敌锋芒, 待机破敌" *"bidi fengmang, daiji podi"*}. Within the entire campaign operations process, [the JCC] always must implement the principles of active use of troops, preemption of the enemy, and active attack, **[end of page 294]** and from start to finish implement initiative-based attack {*zhudong jingong*} and active protection. In the preliminary operations {*xianqi zuozhan*} phase, he must apply various means to ascertain the enemy disposition {*bushu*}. When seizing information dominance, he must use attack as primary; lay stress on key points; and use means and activities such as electronic jamming {*dianzi ganrao*}, computer attack {*jisuanji gongji*}, network

infiltration {*wangluo shentou*}, psychological operations [PSYOPS] {*xinli zuozhan*}, and precision strike {*jingque daji*}, to execute full-dimensional attacks {*quanfangwei gongji*} on the enemy, paralyze the enemy C2 systems, cause enemy electronic facilities equipment to fail {失效 *shixiao*}, and cause radar confusion and blinding {迷盲 *mimang*} and communication interrupts {*tongxin zhongduan*} — to ensure our freedom of activities {*xingdong ziyou*} within the entire battlespace, and create favorable conditions for seizing air dominance/supremacy and sea dominance, as well as for the ground units' activities. While organizing information attack, he should actively adopt protective measures to ensure that friendly {*jifang*} information systems are not sabotaged {*pohuai*} by the enemy; he must synthetically apply methods such as hiding and evasion {*yinni guibi*}, jamming screening {*ganrao yanhu*}, and deceptive secrecy {*qipian baomi*}, and synthetically apply "soft" and "hard" electronic means to do a good job of the counter-reconnaissance {*fanzhencha*}, counter-jamming {*fanganrao*}, counter-espionage {*fandiebao*}, and counter-secrets-leak {*fanxiemi*} work—to ensure the normal operation of our reconnaissance and early warning systems, command communication {*zhihui tongxin*} system, and high-tech weapons systems. He must correctly process the relationship between attack and defense; when seizing information dominance and assisting-supporting the units' operational activities, actively conduct information attack activities; and in order to protect friendly systems against strikes, all along implement protection from start to finish.

IV. Adapting to complex environments, and thoroughly organizing support…295

IO has a high degree of reliance on comprehensive support — intelligence, communication, engineering, technical, and logistics {*houqin*}. An island offensive campaign must focus on the requirements for attack and defense combined {*gongfang jianbei*}, for soft and hard [kill] combined {*ruanying jiehe*}, and for integrated network and electronic [warfare, INEW] {*wangdian yiti*}; lay stress on key points; thoroughly plan and closely coordinate; and conscientiously enhance the comprehensive support capability for IO. First is the need to lay stress on intelligence support. Intelligence is the fountainhead of IO, and without intelligence there would be no operational targets. [We] must, based on the general resolution {*zongti juexin*} for the island offensive campaign, on the guidance thought {*zhidao sixiang*} for IO, and on the mission(s), establish an intelligence network which is vertically linked up {*zongxiang guantong*} and horizontally integrated {*hengxiang ronghe*}, and which [enables] information sharing among all services and arms and at all levels — to timely provide intelligence support {*zhichi*} for joint operations. Second is the need to lay stress on information technology [IT] {*xinxi jishu*} support, with INEW as the core. Electronic warfare [EW] {*dianzizhan*} platforms and computer networks all are the targets of first choice {*shouxuan mubiao*} for the enemy's information key point attacks. Due to the vulnerability of the EW platforms **[end of page 295]** and computer networks themselves, once we suffer enemy strikes and sabotage, even if personnel and weapons are not harmed, we thus could be unable to organically link them into an integrated whole and could lose the proper operational capability. To this end, [we] must put INEW technical support in an important position within IO, and based on the campaign intention, adopt the distributed network-type

deployment mode {*fenbushi wangzhuang peizhi fangshi*}, adjust {*tiaozheng*} the information system strength [force] arrangement structure {*liliang buju jiegou*}, and organize a highly integrated {*yitihua*} technical support contingent — ensuring that under circumstances where some systems are damaged, [we] can in good time [effect] rush repairs and servicing {*qiangxiu weihu*}, to ensure the normal operation of the information systems. Third is the need to lay stress on military-civilian integrated {*junmin yitihua*} support. In view of the characteristic of the arduousness of island offensive campaign IO support missions, [we] must achieve a mutual combination [of military strengths] with local strengths; fully exploit local manpower and material resources; compose a military-civilian integrated IO support net; join into an organic whole the various IO strengths, for intelligence, communication, engineering, technology, and logistics; and thus form comprehensive support superiority, to provide IO with inexhaustible technical and talent support {*zhichi*}.

V. Centering on campaign requirements, and applying multiple means…296

In island offensive campaign IO, the IW is sharp; there is mutual correlation {*xianghu guanlian*} and link-by-link mutual connection {环环相扣 *huanhuan xiangkou*} among the information systems and among all essential factors within the systems, and they operate {*yunzuo*} synchronously with the weapons and equipment {*wuqi zhuangbei*}. These characteristics have determined that IO in terms of strength application must center on the campaign's overall requirements and the IO missions; synthetically apply multiple fighting methods and tactical and technical means to achieve a mutual combination of professional strengths and nonprofessional strengths, a mutual combination of military and civilian strengths, and a mutual combination of standard {制式 *zhishi*} equipment and instrument equipment {*zhuangbei qicai*} and non-standard equipment and expedient materials {*jiubian qicai*}; and form integrated-whole operational effectiveness, to ensure the security of our campaign information and information systems. First, in terms of information acquisition, is the synthetic application of multiple means and multiple channels. The informationized battlespace is vast, the information flow is rapid, the flow volume is sharply increased, and the situations are changeable; seizing the campaign initiative in an even greater way relies on the timely acquisition and effective control of battlefield information. Hence, [the JCC] must in multiple dimensions and 3-dimensionally {*duowei, liti*} disposition the surveillance strengths {*jianshi liliang*}; adopt the mode of a mutual combination of active detection {*zhudong tance*} and passive reception {*beidong jieshou*} and mutual complementation {*xiang buchong*} of technical reconnaissance {*jishu zhencha*} and manual observation {*rengong guancha*}; and exploit means such as communication, **[end of page 296]** radar, and EO reconnaissance {*tongxin, leida, guangdian zhencha*} and computer network reconnaissance, to grasp the operational posture {*zuozhan taishi*} in an all-around, integral, and real-time manner {*quanmian, wanzheng, shishi di*}. Second, in terms of information attack, is flexible application of soft and hard means. He must center on sabotaging and striking at the enemy information systems; take vital site targets such as C2 centers, communication hubs, and radar stations as the key points; and adopt "soft-kill" {*"ruan shashang"*} means such as electronic jamming, electronic deception {*dianzi*

qipian}, virus attack {*bingdu gongji*}, and virtual operations {*xuni zuozhan*} — mutually combined with "hard-destruction" {*"ying cuihui"*} means such as conventional fire strike, force-strength sabotage-raid {*bingli poxi*}, and EM pulse [EMP] attack {*dianci maichong gongji*}, as well as precision fire strike — to execute attacks from the land, sea, air, space, and EM multidimensional space against the enemy's integrated {*yitihua*} command information system; and [thus] accomplish integration of soft and hard means, integration of offensive and defensive operations, and integration of multidimensional {*duowei*} activities. He must lay stress on bringing into play the enormous might {*weili*} of people's war {*renmin zhanzheng*}, and organize the local IO strengths in executing network attacks against the enemy's military, economic, and political information systems, and in disrupting their political, economic, and financial order {*zhixu*}. Third, in terms of information protection, is integrated application of defense, resistance, and counterattack means {防抗反手段 *fang kang fan shouduan*}. While emphasizing offensive subduing of the enemy {*gongshi zhidi*}, he [should] adopt scientific and flexible means to rigorously {*yanmi*} organize information protection, and conscientiously boost the survivability {*shengcun nengli*} of the information systems. He must, based on the battlefield posture {*zhanchang taishi*}, adopt multiple tactical and technical means, including concealment, deception, and disruption {藏, 骗, 扰 *cang, pian, rao*}, to deceive, confuse, and attrite {*xiaohao*} the enemy. He must strengthen computer network system management, defend against enemy network infiltration and virus intrusion, and establish multiple backup systems {*fushi beiyong xitong*} for core computer networks, to ensure the normal operation of the core computer networks. He must effect a multilevel, multiplatform decentralized deployment {*shusan peizhi*} of campaign information systems, in good time organize their mobile transfer {*jidong zhuanyi*}, and use decentralization and maneuver to resist disruption and resist destruction {*kangrao kanghui*}.

Section 3: Island Offensive Campaign IO Activities…297

Island offensive campaigns usually are partitioned into a preliminary operations phase, landing operations {*denglu zuozhan*} phase, and on-island operations {*daoshang zuozhan*} phase. Within an island offensive campaign, the IO activities will **[end of page 297]** penetrate every phase and time segment of the island offensive campaign, to create favorable conditions for seizing victory in the campaign.

I. IO in the preliminary operations phase…298

The JCC {*lianhe zhanyi zhihuiyuan*} and his command organ {*zhihui jiguan*} should organize uninterrupted {*bujianduan*} IO reconnaissance, synthetically apply the campaign's directly subordinate IO strengths and those of the various services and arms, and do all they can to seize information dominance in the main direction, key point areas, and critical time segments, to assist-support and complement {*peihe*} the other operational activities.

When seizing information dominance, [the JCC and command organ] should synthetically apply air, ground, and sea electronic jamming strengths and network attack strengths to execute fierce information attacks against the important targets within the enemy's reconnaissance and early warning systems, C2 systems, communication systems, anti-missile interception {*fandao lanjie*} systems, and electric power supply systems. [They should] apply means such as anti-radiation weapons {*fanfushe wuqi*}, special IW weapons {*teshu xinxizhan wuqi*}, long-range precision guided munitions [PGMs] {*yuancheng jingque zhidao wuqi*}, and special sabotage-raids {*tezhong poxi*}, to carry out key point destruction and sabotage of the enemy's information infrastructure and important information system targets, and to timely conduct jamming and sabotage of newly detected enemy concealed information system targets. [They should] apply multiple means, including electronic camouflage {*dianzi weizhuang*}, information diversion {*xinxi yangdong*}, and EM harassing attacks {*dianci xirao*}, to conduct comprehensive information deception {*xinxi qipian*} against the enemy, and under complementation by other operational strengths, seize campaign local information dominance.

When seizing air dominance/supremacy, [the JCC and command organ] should synthetically apply multiple IO strengths on the ground, in the air, and at sea, to assist-support and complement the operational activities for seizing air dominance/supremacy. During assisting support to conventional missile strike {*changgui daodan tuji*} operations, they should synthetically apply means such as electronic jamming and anti-radiation weapon attacks, to jam and suppress and destroy or sabotage {*cuihui pohuai*} the enemy early warning and detection systems and anti-missile weapons control systems which pose threats to our missile penetration {*tufang*}, so as to assist-support and complement the missile strike activities. During assisting support to air offensive operations {*kongzhong jingong zuozhan*}, they should synthetically apply multiple IO means, and use active information attack activities, to jam and suppress and destroy or sabotage the enemy's air defense early warning {*fangkong yujing*} systems, command guidance {*zhihui yindao*} systems, identification friend or foe [IFF] {*diwo shibie*} systems, and air defense weapons control systems — to complement the other operational strengths, open up penetration corridors {*tufang zoulang*} for the strike force-strengths {*tuji bingli*}, and assist-support the air strike {*kongzhong tuji*} activities of aviation forces {*hangkongbing*}. **[end of page 298]** At the same time, they will apply network attack means to attack the network systems of the enemy's air defense and anti-missile SoS {*fangkong, fandao tixi*}, and to disrupt or sabotage their network system functions {*gongneng*}.

When seizing sea dominance, [the JCC and command organ] should concentrate use of Army, Navy, and Air Force IO strengths, as well as special operations force-strengths {*tezhong zuozhan bingli*}; apply EW aircraft, ground high-power jamming systems and aircraft {*ji*}, and shipborne self-defense EW equipment {*jianzai ziwei dianzizhan zhuangbei*}, to conduct effective jamming and suppression and fire strikes against the important electronic information systems within the enemy stationing and mooring zones (sea zones) {*zhubo di (hai) yu*} and within the at-sea formations

{*haishang biandui*}, as well as against the guidance systems {制导系统 *zhidao xitong*} of air-to-ship and ship-to-ship missiles {*kongduijian, jianduijian daodan*}; and apply network attack means to attack the network systems of the enemy naval operations SoS {*haishang zuozhan tixi*}, and to disrupt and sabotage their functions.

When seizing and occupying {*duozhan*} and blockading the enemy-held outer islands {*waiwei daoyu*}, [the JCC and command organ] should in good time organize and command the IO strengths to conduct jamming and suppression or destruction and sabotage of command centers, communication hubs, and reconnaissance and early warning systems in the navigational crossing sea zones {*hangdu haiyu*}, so as to assist-support and complement the operational activities of the offshore {*jin'an*} operational groups in seizing and controlling {*duokong*} the enemy-held outer islands.

When the enemy conducts counter-preemption operations, they should in good time organize and command the IO strengths to conduct jamming and suppression of the enemy C2 systems, air raid weaponry {*kongxi bingqi*} information systems, and navigation positioning {*daohang dingwei*} systems, to assist-support and complement our other strengths in conducting resistance and protection operational activities. They also should synthetically apply information defense means to strengthen information protection for important C2 systems, communication hubs, radar positions {*leida zhendi*}, missile positions {*daodan zhendi*}, and airfield navigation systems, to screen the safety of our important information targets.

Over the entire process of preliminary operations, they should fully exploit propaganda means such as operations releases {*zhankuang fabu*}, radio, and TV, and psychological warfare [PSYWAR] weapons {*xinlizhan wuqi*}, to execute powerful psychological attacks on the enemy, break up the enemy troops' morale, and disintegrate the enemy will; and they should flexibly organize information defense activities, to ensure our operational INFOSEC and the bringing into play of the information systems' effectiveness.

II. IO in the landing operations phase…299

The JCC and his command organ should synthetically apply multiple IO **[end of page 299]** strengths and means, to conduct key point jamming and suppression and destruction or sabotage of information system targets — for enemy reconnaissance and surveillance [R&S] {*zhencha jianshi*}, command communication, and air defense and anti-missile weapons control — in our main navigational crossing direction and the important landing sectors {*denglu diduan*}, to assist-support and complement our landing operations activities.

When the landing operations groups adopt multiple modes for rapid assembly onto the ships {*jijie shangchuan*}, [the JCC and command organ] should strengthen surface-to-air and anti-surface {*duikong, duihai*} IO reconnaissance, to rapidly ascertain the situation of the enemy electronic information targets after the preliminary strikes; and

they especially must strengthen reconnaissance {侦控 *zhenkong*} of newly detected electronic information targets. They also should at the right time organize and conduct electronic diversion/demonstration {*dianzi yangdong*}, set up false electronic targets {*shezhi jiadianzi mubiao*}, and conceal the true while displaying the false {*yinzhen shijia*}, to confuse and deceive the enemy, and to screen the activities of assembly onto the ships. At the same time, they must adopt multiple INFOSEC secrecy {*xinxi anquan baomi*} measures, and strictly control EM radiation {*dianci fushe*} in the zones for assembly onto ships, to conceal the operational intention {*zuozhan qitu*}.

When the landing operations groups get underway at sea {*haishang hangdu*}, [the JCC and command organ] should use the air and sea IO strengths as primary, and adopt the method of a mutual combination of area (zone) screening {*quyu yanhu*}, escort cover {*bansui yanhu*}, and self-defense screening {*ziwei yanhu*}, to screen the activities of the landing transportation formations {*denglu shusong biandui*}. In the diversionary navigational crossing {*yangdong hangdu*} direction, they [should] synthetically apply multiple electronic deception means, including electronic jamming and electronic camouflage, to complement other campaign diversion measures, simulate {*moni*} navigational crossing and escort formations {*huhang biandui*}, and conduct information deception against the enemy, to give the enemy false impressions and to attract and contain {钳制 *qianzhi*} the enemy anti-landing force-strengths {*kangdenglu bingli*}, so as to screen the landing activities in the main direction. In the main navigational crossing direction, they [should] organize sea and air electronic attack [offensive] {*dianzi jingong*} strengths, to jam and sabotage the enemy R&S systems, so as to preserve the concealed quality {*yinbixing*} of the navigational crossing, and to jam and suppress the enemy's fire strike control systems, so as to degrade their strike effectiveness, and provide effective cover for our navigational crossing formations.

When the landing operations groups conduct a multipath 3-D landing, [the JCC and command organ] should use air IO strengths as primary, and simultaneously use multiple means for key point jamming and sabotage of enemy command communication, coordination communication {*xietong tongxin*}, gun position target search fire adjustment radar {*paowei zhencha jiaoshe leida*}, gun aiming radar [fire control radar] {*paomiao leida*}, missile guidance radar {*daodan zhidao leida*}, and radio fuses [detonators] {*wuxiandian yinxin*} within the areas (zones) for assault onto land {*tuji shanglu quyu*}, so as to assist-support our landing units' activities in the assault onto land.

When resisting land-sea-air joint counterattack {*luhaikong lianhe fanji*} executed by enemy reserve forces {*yubeidui*}, and consolidating and enlarging the campaign landing field(s), [the JCC and command organ] should use air electronic attack strengths and ground high-power electronic jamming means as primary, with the key points on conducting jamming and suppression of the command communication and coordination communication of the enemy's joint counterattack forces. **[end of page 300]** They also should apply means such as operational and tactical missile {*zhanyi zhanshu daodan*} and aviation firepower, to strike at enemy command centers and communication hubs,

and cause them difficulty in organizing effective counterattack activities, so as to assist-support and complement the landing units' capture {*duozhan*} and enlargement of the campaign landing field(s).

Over the entire process of the landing operations, they should apply means such as network infiltration attack {*wangluo shentou gongji*}, denial-of-service [DoS] attack {*jujue fuwu gongji*}, virus attack, and e-mail attack {*youjian gongji*}, to execute attacks against the network systems of the enemy's anti-landing operational SoS, and weaken their functions. They should fully exploit propaganda media such as operations releases, radio, TV, and newspapers and magazines, and PSYWAR weapons — and combine these with means such as distributing leaflets {*sanfa chuandan*} and battlefield propaganda directed at the enemy {战场喊话 *zhanchang hanhua*} — to execute sustained {*chixu*} psychological attacks against the enemy, and to shake the enemy army's morale {*di junxin*} and weaken the enemy's morale {*di shiqi*}, so as to complement the activities of the other operational strengths. They should synthetically adopt technical and tactical measures to thoroughly organize information defense, so as to support landing operations INFOSEC and the normal bringing into play of the information systems' effectiveness.

III. IO in the on-island operations phase…301

The JCC and his command organ should use ground and air information attack strengths as primary; synthetically adopt means such as EM interdiction {*dianci zheduan*}, network attack, and psychological attack, and combine these with firepower destruction and force-strength sabotage-raid activities, to jam and sabotage the information systems of the enemy they face; and flexibly organize information defense activities, to ensure that the on-island operations information systems normally bring into play their operational effectiveness, and to create favorable conditions for the attack units to annihilate {*jianmie*} the defending enemy.

When the on-island offensive units launch the attack, [the JCC and command organ] should organize the electronic attack strengths, to effect key point jamming and suppression of the facing enemy's radio/wireless command communication {*wuxiandian zhihui tongxin*}, coordination communication, and gun position target search fire adjustment radar, and carry out anti-radiation destruction of radar in the enemy's rear-area missile positions. When engaging with the enemy's deep units {*zongshen budui*}, they should timely employ ground and air EW reserve strengths, for key point jamming and suppression of the enemy's command communication and coordination communication, to complement the operational activities of the rapid assault units {*kuaisu tuji budui*}. [Finally,] when annihilating the encircled enemy, they should put the key points on interdicting the encircled enemy's radio/wireless signal communication {*wuxiandian tongxin lianluo*} with the outside, and jamming and suppressing their weapons control systems, to assist-support the surrounding and annihilation {围歼 *weijian*} operational activities. **[end of page 301; end of chapter]**

This page intentionally left blank.

Chapter 18
Border Defense Campaign {*bianjing fangyu zhanyi*} Information Operations…302

Border defense campaigns are defensive-quality {*fangyuxing*} campaigns conducted in a border area {*bianjing diqu*} in order to maintain {*weihu*} national sovereignty, territorial integrity, and security. In border defense campaign information operations (IO), since they are subject to the influences and restrictions of multiple subjective and objective factors {*yinsu*} such as the social and human, natural geographic, and installation [facility] technical {*sheshi jishu*} [factors], the operational environment and missions are unusually complex and arduous, and seizure of battlefield information dominance {*zhixinxiquan*} will have extremely important influence on the progress {*jincheng*} and outcome {*jieju*} of the campaign.

The main missions of border defense campaign IO are as follows: to conduct IO reconnaissance {*zhencha*}, with the key points {*zhongdian*} on ascertaining in the main direction {*zhuyao fangxiang*} and key point areas situations such as the composition and deployment {*peizhi*} of the enemy's information systems {*xitong*}, including reconnaissance and surveillance (R&S) {*zhencha jianshi*}, command, communication {*tongxin*}, and weapons control {*wuqi kongzhi*}, as well as their technical parameters {*canshu*}; to jam and suppress {*ganrao yazhi*}, and destroy or sabotage {*cuihui pohuai*} the enemy ground and air command and control (C2) systems {*zhihui kongzhi xitong*} and communication systems; to paralyze {*tanhuan*} or delay their operational command {*zuozhan zhihui*}; to assist-support and complement {*zhiyuan, peihe*} border-area operational activities {*zuozhan xingdong*} on land and in the air; and to implement information defense {*xinxi fangyu*}, to ensure our operational information security (INFOSEC) {*xinxi anquan*} and the stable operation {*yunxing*} of our information systems.

Section 1: Characteristics {*tedian*} of Border Defense Campaign IO…302

In a border defense campaign, IO penetrates from start to finish, and can have a major influence on the progress and outcome of the campaign. Within border defense campaigns, IO takes on the following **[end of page 302]** main characteristics.

I. Initial-period battlefield posture {*zhanchang taishi*} is relatively passive, and information defense missions are arduous…303

Border defense campaigns usually are begun under circumstances where the enemy first conducts a local invasion {*jubu ruqin*} against us. The battlefield posture from the viewpoint of the integrated whole {*zhengti*} is one of the enemy attacking while we defend; the enemy has the initiative {*zhudong*}, while we are in a passive position. The enemy, for quite a period of time before conducting the invasion against us and after the invasion begins, will widely employ IO strengths dispositioned {*bushu*} in outer

space {*taikong*}, in the air, and on the ground, to conduct against us full-dimensional {*quanfangwei*}, full-depth {*quanzongshen*}, multi-field {*duolingyu*}, long-duration IO activities with a combination of soft kill {*ruan shashang*} and hard destruction, and a combination of open means and secret means; to carry out jamming and sabotage or destruction of important information targets {*xinxi mubiao*}, such as our C2 centers, air defense systems {*fangkong xitong*}, communication hubs {*tongxin shuniu*}, radar stations, and computer network nodes {*jisuanji wangluo jiedian*}; and to intend in one stroke to paralyze our information systems, and cause our command to go out of order {*shiling*} and our units to go out of control. IO strengths are the most important targets of enemy attacks; and under circumstances where [our] IO equipment {*zhuangbei*} is in the inferior position, integrated-whole {*zhengti*} defensive preparations are not complete, and the enemy holds the initiative of the first opportunity initiative {*xianji zhudong*}, information system protection and INFOSEC secrecy {*baomi*} will be extremely difficult. Hence, in a campaign's early period, IO activities must adopt multiple measures to counter enemy information reconnaissance, counter enemy electronic jamming {*dianzi ganrao*}, defend against enemy special sabotage {*tezhong pohuai*}, and counter the enemy's precision firepower destruction {*jingque huoli cuihui*}; to effectively support {*baozhang*} the transmission {*chuandi*} and use of operational command information; and to support the security and secrecy {*anquan baomi*} of operational information and the stable operation of the operational command information system. [Translator's note: unless otherwise indicated, all "support" in this chapter is "safeguarding support" {*baozhang*}.]

II. The battlefield's natural environment is harsh, and IO is greatly influenced by the environment…303

Border defense campaigns usually are conducted within a certain area on both sides of China's inland border lines; the battlefield geographic environment is complex, and not favorable to our conducting of IO activities. This is mainly expressed in the following: the operational zone {*zuozhan diyu*} roads are few, road conditions are poor, and the battlefield has high and steep mountains; [this zone is] susceptible to enemy sabotage, and is inconvenient for the concealed maneuver {*yinbi jidong*} of our IO strengths. The continuous high mountains easily create signal dead zones {*xinhao jingqu*}, the thunderstorms and sandstorms peculiar to the plateaus have powerful interference effects {*ganrao zuoyong*} on radio signals, information transmission attenuation is high, and signal quality is poor; moreover, there easily appear information blind zones {*xinxi mangqu*}, creating information linkup {*goutong*} difficulties. The climate is unusually cold, so that various types of **[end of page 303]** information facilities equipment {*shebei*} are subject to severe influences, operating systems {*caozuo xitong*} do not work, and instrument and meter indicator data {*zhibiao shuju*} is inaccurate; this degrades the operational capability {*zuozhan nengli*} of some IO personnel and IO equipment {*zhuangbei*}. The civilian-use communication resources cover area {*fugai mian*} is small, and the level of their availability {*kezi liyong chengdu*} is low. Vegetation {*zhibei*} is sparse, targets are exposed, and constructing of fortifications {*gongshi*} is unusually difficult, [all of which are] inconvenient for implementing camouflage {*weizhuang*}. Field survival {*yezhan shengcun*} conditions are poor, making

it difficult to fully bring into play the combat power {*zhandouli*} of the IO units. Safeguarding support and assisting support {*baozhang, zhiyuan*} for IO activities are difficult, so operational activities are limited to being conducted within one thoroughfare or multiple thoroughfares, and mutual information resources sharing {*xinxi ziyuan gongxiang*} is difficult; and the degree of difficulty in organizing command of IO is high.

III. The theater's {*zhanqu*} social environment is complex, and the IO operations-research-based planning {*chouhua*} attention points are numerous…304

Border defense campaigns very likely can be situated in border areas with internal and external troubles {内忧外患 *neiyou waihuan*} simultaneously present. Once border hostilities {战事 *zhanshi*} occur, domestic and foreign terrorists will surely collude internally and externally {内勾外联 *neigou wailian*}; stir up trouble to serve their own ends {趁火打劫 *chenhuo dajie*}, and await an opportunity to create disturbances or riots, and even armed rebellion {*wuzhuang panluan*}; and internally and externally work in concert {内外呼应 *neiwai huying*}, to sabotage the campaign rear's roads, bridges, and information infrastructure {*xinxi jichu sheshi*}, spy out our military secrets {*citan wo junqing*}, assassinate our personnel, and disturb our operations area's popular support and morale, to complement the enemy's battlefront {*zhengmian zhanchang*} operations. Hence, within border defense campaigns, the various contradictions {*maodun*} are sharp {*jianrui*} and complex, and the attention points for seizing local information dominance are numerous. The joint campaign commander {*lianhe zhanyi zhihuiyuan*} not only must pay attention to the sharp electromagnetic (EM) warfare {*dianci duikang*} within the land, air, and space scope {*lu, kong, tian fanwei*}, but also must closely {*miqie*} pay attention to the public opinion trends of the different faiths, different religious sects, and public organizations; he not only must pay attention to the battlefront's enemy information offensives {*xinxi jingong*}, but also must pay attention to sabotage and harassing attacks {*xirao*} by terrorists in the campaign rear against our command information system; and he not only must carry out direct information warfare (IW) {*xinxi duikang*} with the enemy faced, but also must pay attention to possible information intervention {*xinxi ganyu*} activities by third parties.

IV. Battlefield information installations lag behind, IO strength assisting support is difficult…304

In border defense campaigns, the battlefield is far from our deep heartland {*zongshen fudi*}; civilian-use information installations are few, and the IO resources which can be converted are extremely limited. In recent years, although we have built in the border areas a strategic communication net {*zhanlue tongxin wang*} with wired communication and satellite communication {*youxian tongxin, weixing tongxin*} as primary, nonetheless **[end of page 304]** the theater communication and command system {*tongxin zhihui xitong*} mainly is concentrated within the campaign depth. The forward-edge {*qianyan*} communication infrastructure is relatively weak, and the communication means are fairly unitary. The distances between a theater's various campaign directions are more than a hundred kilometers (km); the battlefield's already built airfields and

roads are few, and [the areas] not only lack railways {*tielu*} but also lack air transport {*kongyun*} and water transport; traffic and transport {*jiaotong yunshu*} completely relies on highways, but the highways too have not been formed into a network, so maneuver is limited. Within IO, once the information facilities equipment encounters enemy raids {*xiji*} and [/or] sabotage, the IO strengths' assisting support will be extremely difficult. The information adversary, while strengthening {*jiaqiang*} its tri-service modernization drive, is constantly strengthening the border areas' IO battlefield construction, and has formed a favorable battlefield posture. In border defense campaigns, the missions of IO [thus] will be unusually arduous.

Section 2: Requirements {*yaoqiu*} of Border Defense Campaign IO…305

Border defense campaign IO must tightly center on the campaign intention {*zhanyi qitu*}, and to the maximum extent bring into play the systemic functions {*xitong gongneng*} of all essential factors {*yaosu*} of IO, to seize local information dominance.

I. Scientific organizational grouping {*bianzu*} of strengths, forming an IO integrated-whole composite strength {*zhengti heli*}…305

In border defense campaigns, the battlefield terrain is complex, and the climate and environment are harsh; the enemy situation's {*diqing*} unknown factors are many, and campaign pattern transitions {*zhanyi yangshi zhuanhuan*} are frequent. Hence, [the commander] must scientifically organizationally group and apply the IO strengths, to form an IO integrated-whole composite strength. First is that, in the operational organizational grouping, he should, based on the border defense campaign disposition {*bushu*} and on the IO missions, organizationally group the IO strengths into IO groupings and elements {*qun, dui*} which can adapt to various complex situations. The various groupings and elements then are used for a small sub-grouping {*xiaode fenqun*} or small detachment {*xiao fendui*} task organization {*biancheng*}, to fully bring into play the IO strengths' superiority as fighters with multiple skills {*yibing duoyong*} and as experts in one field while possessing general abilities {*yizhuan duoneng*}, and to accomplish during decentralized activities {*fensan xingdong*} being small targets with strong capabilities, convenient to maneuver and support; and during centralized activities {*jizhong xingdong*}, at the right time flexibly combining, to rapidly form fairly strong IO capabilities. At the same time, the organizational grouping also must embody a combined quality {*hechengxing*}, to ensure a full complement {*qiquan peitao*} of the basic essential elements, including command, reconnaissance, direction finding {*cexiang*}, and jamming, within the groupings and elements, and [to ensure] **[end of page 305]** rationality of communication, technical, logistics, and battlefield rescue {*jiuhu*} support. Second is that in the operational deployment {*zuozhan peizhi*}, he should give precedence to {*youxian*} selecting terrain favorable to bringing into play the performance of the IO force-strengths and weapons {*bingli bingqi*}, and should as much as possible deploy the IO reconnaissance facilities equipment {*zhencha shebei*} in high areas convenient to observation {*guancha*}. The IO jamming facilities equipment should fully exploit favorable terrain, break through the conventional [methods], and [realize]

concealed forward deployment {*yinbi kaoqian peizhi*}, so as to reduce the unfavorable influence of the terrain, and enhance the IO effects {*xiaoguo*}. He must strengthen concealment and camouflage {*yinbi weizhuang*}, to boost the survivability {*shengcun nengli*} of the IO strengths. He must form a network-type disposition {*wangzhuang bushu*}, so that all groupings and elements can fully exploit the favorable terrain to unfold {*zhankai*} the IO activities and achieve the concealment and camouflage goals {*mudi*}. He also should, based on the actual situation of the enemy and friendly sides {*diwo shuangfang*}, organizationally group IO maneuver groupings and elements, and accomplish a mutual combination of centralization and decentralization {*jizhong yu fensan*} and a mutual combination of fixed and mobile {*jidong*}, so as to execute intersecting and multipoint attacks against the enemy's important targets, and enhance the IO effects.

II. In view of the special {*teshu*} environments, bringing into play the role of IO strengths with high maneuverability {*jidong nengli*}…306

In border defense campaigns, the battlefield is rather remote, and the survival environment is harsh. Our IO units in peacetime are difficult to garrison {驻守 *zhushou*} for long periods; in wartime we will mainly rely on temporary transfer {*linshi…choudiao*} from the campaign's shallow depth {浅近纵深 *qianjin zongshen*} of IO contingency maneuver units (elements) {*yingji jidong bu (fen) dui*} injected into operations. Force-strength transportation {*bingli shusong*} and maneuver difficulties will be numerous, their time long, and the enemy air threats faced high. Since the border areas' terrain is complex and the climatic conditions harsh, the IO force-strength and weapons effectiveness {*xiaoneng*} will be restricted. Hence, the joint campaign commander and his command organ {*zhihui jiguan*} must fully bring into play the role of IO strengths with high maneuverability. Provided that conditions permit, they should build an IO system of systems {*tixi*} with an outer space, air, and ground triad {*sanwei yiti*}, and apply air IO strengths and high-maneuverability {*jidongxing qiang*} ground IO strengths, in the main direction and important time segments {*shijie*}, to conduct jamming and suppression of vital site positions {*yaohai buwei*}, such as the enemy's C2 centers, information processing centers, communication and computer centers, and early warning and detection system nodes {*yujing tance xitong jiedian*}, and to cause interrupts {中断 *zhongduan*} in enemy operational information, thus leading to command paralysis, coordination imbalance {*xietong shitiao*}, and weaponry going out of control {*bingqi shikong*}. **[end of page 306]**

III. Extraordinary employment {*chaochang shiyong*} of strengths, forming local IO force-strength superiority {*bingli youshi*} over the enemy…307

The joint campaign commander and his command organ must aim at the border areas' special geographic environments and at the missions and requirements of the border defense campaign, and extraordinarily reinforce the IO strengths. In particular, they must increase the organized and allocated proportion {*bianpei bili*} of IO strengths in the main direction and important areas, to ensure that the IO strengths in the

campaign's important phases and critical time segments are adequate and effective {*guanyong*}. To this end, first is that they must adopt the methods of mutual combinations of level-by-level reinforcement {*zhuji jiaqiang*} and bypassing reinforcement {*yueji jiaqiang*}, and of fixed-point reinforcement and accompanied reinforcement {*bansui jiaqiang*}; bypass the organizational system {*chaoyue jianzhi*}; and select and use the elite {*jingrui*}, to form an IO crack force of elite troops {精兵劲旅 *jingbing jinglyu*} which can effectively compete with the enemy, and in the limited operational space {*zuozhan kongjian*} bring into play its role to the maximum extent. Second is that they must concentrate their employment, and form key points. Concentrated strengths and key point strikes are a general rule of all operations. The joint campaign commander and his command organ must aim at the needs and requirements {*xuyao*} of border defense campaign IO, and within a certain operations area (zone) {*zuozhan quyu*} and time domain {*shiyu*} or frequency domain {*pinyu*}, concentrate employment of the various IO strengths; use IO weapons and equipment of different dimensions {*fangwei*}, different depth, and different power levels {*gonglyu*} to form jamming and strike superiority over the enemy's important electronic targets. Third is that they must select important information targets, those which can produce the maximum influence on the enemy's integrated-whole operational effectiveness {*zhengti zuozhan xiaoneng*}, for executing the key point strikes, so as to weaken the enemy's integrated-whole IO capability.

IV. Laying stress on military-civilian combination {*junmin jiehe*}, to bring into play the integrated-whole might {*zhengti weili*} of military-[armed] police-militia {军警民 *jun jing min*} IO…307

The Information Age has entrusted traditional people's war {*renmin zhanzheng*} with new connotations, and has provided the best opportunity for bringing into play its might. In view of the grave circumstances {形势 *xingshi*} of enemy strength and our weakness in informationized {*xinxihua*} weapons and equipment, if we desire to gain success in border defense campaign IO under future informationized conditions, we must firmly and unshakably carry on and develop the thought of people's war, and fight IW {*xinxizhan*} on the basis of a people's war. First is that we must as rapidly as possible establish mass {*qunzhongxing*} IO organizations, and bring into play the roles of the multiple strengths of the militia {*minbing*} and the masses, and from different directions and different fields conduct information offensives against the enemy. Second is that we must fully exploit local {*difang*} information installations. For example, information systems have strong universality {*tongyongxing*}: the military-civilian jointly built fiberoptic cable transmission net {*guanglan chuanshu wang*} **[end of page 307]** has many network stations {*wangluo zhandian*} and control centers, all of which are military-civilian combined and military-civilian integrated {*jundi yiti*}. We should fully rely on and bring into play the role of these local information installations and information resources. Third is that we must adopt multiple simple and easily implemented, military-civilian general purpose fighting methods {*zhanfa*}. Examples include adopting the method of a mutual combination of modern information means and traditional information means, and, via large-quantity dissemination {*sanbu*} into public opinion of

information unfavorable to the enemy, containing and driving a wedge into {*qianzhi, lijian*} the enemy's activities; and adopting the method of a mutual combination of professional {*zhuanye*} IO strengths and non-professional {*feizhuanye*} IO strengths, and via multiple avenues, conducting population-wide {*quanminxing*} IO in a multidimensional {*duofangwei*}, multi-field, full-time/space {*quanshikong*} manner.

V. Attack and defense simultaneously developed {*gongfang bingju*}, using attack to aid defense, striving for local information superiority {*jubu xinxi youshi*}…308

In border defense campaign IO, our information offensive means are limited, the information acquisition scope is small and the channels are few; the entire border area's existing information infrastructure and information resources have a low level of availability {*kezi liyong chengdu*}, its information strengths are thin, and the overall information offensive capability still is fairly weak. However, in the enemy faced, the technical levels {*shuiping*} of IO equipment, including early warning [systems], electronic reconnaissance {*dianzi zhencha*} and electronic jamming [systems], and computer network systems, are high, and his IO capability is strong. Hence, an overall posture where the enemy is strong and we are weak has decided that we do not possess the capability for conducting IW in the full time domain and full space domain with the enemy. Only by first employing active defense {*jiji fangyu*}, and to the maximum extent reducing the degree of damage {*huishang chengdu*} by the enemy to our information and information systems, and preserving our IO strengths, will we then be able to execute effective offensives against the enemy in the key point direction and critical time segments. On one hand, we must focus on an early-stage posture {*chuqi taishi*} where the enemy faced has strong information reconnaissance capability and high jamming power, and where in equipment performance the enemy is superior and we are inferior; employ all-around, effective information defense to conceal our maneuver routes, force-strength assembly {*bingli jijie*}, and true intentions; and at the same time support the bringing into play of the normal operating effectiveness {*gongzuo xiaoneng*} of our information facilities equipment, to lay the foundation for using effective information defense for an information offensive. On the other hand, we must, from the viewpoint of contending for {*zhengduo*} information dominance, select favorable time opportunities {时机 *shiji*} to conduct information attacks {*xinxi gongji*} against the enemy's command communication system, radar stations, and computer network nodes; reduce or halt {减煞 *jiansha*} the enemy's information offensive capability; and preserve the stability of our border defense SoS, so as to create favorable conditions for seizing victory in the border defense campaign. **[end of page 308]**

Section 3: Border Defense Campaign IO Activities…309

Border defense campaigns usually are divided into three phases: defensive operations {*fangyu zuozhan*}, counterattack {*fanji*} operations, and concluding the campaign. Border defense campaign IO will center on the main operational activities of these three phases, comprehensively apply {*zonghe yunyong*} various IO strengths, and use multiple effective IO activities and measures to contend for battlefield information

dominance, so as to ensure creating the conditions for the smooth implementation of the border defense campaign.

I. IO in the defensive operations phase…309

The joint campaign commander and his command organ should comprehensively apply multiple IO strengths to conduct reconnaissance, jamming, destruction, and [/or] sabotage against critical positions {*guanjian buwei*} and vital site targets {*yaohai mubiao*} of the enemy's important information systems, such as those for R&S, C2, and communication, and to contend with the enemy for battlefield local information dominance.

When the enemy conducts an information offensive, they should comprehensively apply multiple information defense means and measures to take enemy entity destruction {*shiti cuihui*} as the key point, and to take command centers, communication hubs, and radar stations as the main protection targets, and adopt the modes of concealment and camouflage and setup of false targets {*shezhi jiamubiao*}, to decentralize the enemy's information offensive, and to boost the counter-destruction capability {*kanghui nengli*} of information system targets. In good time, [they also should] organize counter-reconnaissance {*fanzhencha*}, counter-jamming [jam-resistance] {*fanganrao*}, and counter-network-attack {*fanwangluo gongji*} activities, to ensure the normal realization of our electronic information systems' effectiveness.

When the enemy conducts preliminary firepower strikes {*xianqi huoli daji*}, they should concentrate use of the electronic jamming strengths, for key point jamming and suppression of the enemy's airborne fire control systems {*jizai huokong xitong*}, ground mobile {*dimian huodong*} target reconnaissance radar, and gun position target search fire adjustment radar {*paowei zhencha jiaoshe leida*}, as well as missile guidance systems {*daodan zhidao xitong*}, to reduce the enemy fire assault {*huoli tuji*} effects.

When we conduct holding [staunch defense] operations {*jianshou zuozhan*}, [the joint campaign commander and his command organ] should comprehensively employ the IO strengths of the Army, Air Force, and Second Artillery Corps, as well as special operations force-strengths, for key point jamming and sabotage of enemy reconnaissance and detection {*zhencha tance*}, **[end of page 309]** weapons control, and radio/wireless communication systems {*wuxiandian tongxin xitong*}, to assist-support the defensive units' holding [staunch defense] operational activities; and they should timely grasp the situation of important electronic information facilities equipment which have suffered enemy jamming and [/or] sabotage, and adopt active information defense measures to ensure the normal operation of the main electronic information facilities equipment.

When we conduct anti-air landing operations {*fankongjiang zuozhan*}, they should use the campaign reserve forces' {*zhanyi yubeidui*} IO strengths as primary, under the assisting support and complementation {*zhiyuan peihe*} of other IO strengths, for key point jamming and suppression of the command communication and coordination

communication {*xietong tongxin*} of the enemy air landing in our campaign depth, and to assist-support the anti-air landing operational activities.

At the same time, over the entire process of defensive operations, they should apply network attack strengths, to execute attacks against the enemy's battlefield network systems, to degrade the enemy's operational command effectiveness; exploit many types of public opinion propaganda and psychological warfare (PSYWAR) weapons {*xinlizhan wuqi*}, to execute psychological attacks against the enemy, and to complement the other units' defensive operational activities; and adopt multiple measures to enhance the psychological protection of the participating {*canzhan*} personnel, and to preserve the units' exuberant will to fight.

II. IO in the counterattack operational phase…310

IO activities in the counterattack operational phase mainly provide IO assisting support for conducting the operational activities, including integrated fire assault {*zonghe huoli tuji*}, outflanking envelopment {*yuhui baowei*}, continuous cutting apart and annihilation {*lianxu gejian*}, land-air joint counterattack, and search and suppression and pursuit and attack {*soujiao yu zhuiji*}. The joint campaign commander and his command organ should organize information reconnaissance strengths to conduct reconnaissance against the enemy, and timely grasp the operating situation of the predetermined counterattack targets' radio/wireless command communication, gun position target search fire adjusting radar, and missile guidance systems and electro-optical (E-O) systems {*guangdian xitong*}; organize electronic jamming and diversion {*dianzi ganrao yangdong*}, to complement the other campaign activities, deceive and confuse {*qipian mihuo*} the enemy, and screen the main counterattack direction's operational activities; and use ground and air electronic jamming strengths as primary, for key point jamming and sabotage of important targets in the enemy's battlefield information system, so as to create favorable conditions for assisting-supporting and complementing the counterattack operational activities of the other operational strengths.

When executing an integrated fire assault against the enemy, they should concentrate use of information offensive strengths, **[end of page 310]** and coordinate with aviation forces {*hangkongbing*} and artillery units {*paobing budui*}, to effect jamming and destruction of the counterattack targets' radio/wireless command communication, coordination communication, gun position target search fire correction radar, and missile guidance systems, to weaken their operational capability. When conditions permit, they [can] use means such as operational and tactical missiles {*zhanyi zhanshu daodan*}, anti-radiation missiles (ARMs) {*fanfushe daodan*}, high-power microwave (HPM) weapons {*gaogonglyu weibo wuqi*}, and EM pulse bombs (E-bombs) {*dianci maichong zhadan*}, to attack the enemy electronic information system's important targets; and [can] dispatch special operations elements {*tezhong zuozhan fendui*}, carrying IO weapons such as portable {*bianxieshi*} EM jamming facilities equipment and directed energy weapons (DEWs) {*dingxiang neng wuqi*}, to infiltrate

{*shentou*} into the enemy depth, and execute short-distance {*jinjuli*} information attacks against the enemy information system's critical nodes and vital site positions.

When conducting outflanking envelopment and continuous cutting apart and annihilation of the enemy, they should concentrate use of IO strengths with high land (sea) and air maneuverability, to accompany the counterattack units in conducting jamming of the enemy, and to assist-support the outflanking envelopment and continuous cutting apart and annihilation operational activities. The land electronic offensive strengths should [effect] key point jamming and suppression of the enemy reconnaissance, guidance radar, and command communication systems, to screen the land counterattack activities. The air electronic offensive strengths should [effect] key point jamming and suppression of the various types of radar within the enemy's field air defense system {*yezhan fangkong xitong*}, to assist-support the strike activities {*tuji xingdong*} of the aviation force attack formations {*gongji biandui*}.

When executing a land and air joint counterattack against the enemy's follow-up echelons {*houxu tidui*}, the land electronic offensive strengths [effect] key point jamming and suppression of the facing enemy's radio/wireless communication and battlefield radar targets. The air electronic offensive strengths [effect] key point jamming and suppression of important electronic information targets in the main direction's enemy depth, and assist-support and complement the land and air joint counterattack groups in executing encirclement {*hewei*} and cutting apart and annihilation of the pre-annihilated {预歼 *yujian*} enemy.

During search and suppression and pursuit and attack operations, [the joint campaign commander and his command organ] should command IO strengths to [conduct] key point jamming and suppression of the command communication and coordination communication of the enveloped remnant enemy, and sever their communication contact with the outside.

Over the entire process of counterattack operations, they also should in good time apply network attack means to sabotage the enemy's battlefield network system functions; exploit multiple psychological attack means to cause fear in the enemy, **[end of page 311]** to weaken his will to resist, and to assist-support and complement the other operational strengths' counterattack operational activities; and adopt multiple measures to flexibly organize and implement information defense, to ensure the normal realization of our counterattack operational information system's effectiveness, as well as operational INFOSEC.

III. IO in the concluding the campaign phase…312

The border defense campaign operations' conclusion means the activities when the operational goals are already basically achieved, or when it is required to transition the operational mission. The joint campaign commander and his command organ should

comprehensively apply multiple IO means to continue maintaining battlefield local information dominance, and to screen the units' safe withdrawal from the battlefield.

When we withdraw from the battlefield, they should concentrate employment of information offensive strengths to conduct intense blanket jamming {*yazhi ganrao*} of enemy electronic information targets in areas facing us and along our withdrawal route, as well as in the two flanks' areas (zones) {*liangyi quyu*} and in the shallow depth within the air zone {*kongyu*}, and in particular, conduct effective jamming and suppression of the enemy's space-based reconnaissance systems {*tianji zhencha xitong*}, to confuse and blind {迷盲 *mimang*} the enemy reconnaissance and detection systems, so that the enemy has difficulty perceiving our withdrawal activities. At the same time, [the commander and command organ] must organize electronic offensives in different directions, to create the false impression that we will again launch an offensive {*fadong gongshi*}, to cause the enemy to produce erroneous assessments of our intention, and to force him to implement defensive activities preparations. Electronic protection strengths should place key points on doing a good job of the EM protection work along the maneuver way of our critical targets. Anti-radiation attack strengths should execute concentrated suppression and destruction of enemy EM radiation sources {*dianci fushe yuan*} posing a fairly high threat, and at all times prepare to execute attacks and destruction against EM radiation sources carried by the enemy tailing behind our military, to delay his activities speed.

When forming a new defensive SoS, information offensive strengths should continue to conduct large-scope blanket jamming of the enemy's deep reconnaissance and detection systems, to screen our operational groups {*zuozhan jituan*} constructing new defensive positions {*fangyu zhendi*}, and timely forming of a new defensive SoS. The anti-radiation attack strengths should resolutely destroy [any] newly appearing IO targets, such as newly built radar stations, reconnaissance and early warning aircraft {*zhencha yujing feiji*}, and mobile jamming platforms, which pose a fairly high threat to us. The electronic protection strengths should employ multiple means, such as false positions, false fortifications, and EM decoys {*dianci youer*}, to boost the EM protection capability of our important targets, and use active electronic offensive {*dianzi gongshi*} activities to at all times answer **[end of page 312]** the long-range precision strike {*yuancheng jingque daji*} activities which the enemy can launch.

In the concluding the campaign phase, the PSYWAR and network warfare {*wangluozhan*} strengths should increase the sabotage level of force {*pohuai lidu*}, and employ multiple broadcast media {传媒 *chuanmei*} means internationally and domestically to create public opinion favorable to a stable battlefield situation, to consolidate and strengthen our military's psychological superiority at the confrontation forward edge {*duizhi qianyan*}, and to force the enemy to not dare again act rashly and recklessly {轻举妄动 *qingju wangdong*}. **[end of page 313; end of chapter]**

This page intentionally left blank.

Chapter 19
Air Defense Campaign Information Operations…314

An air defense campaign {*fangkong zhanyi*} is a defense-counterattack integrated {防反一体 *fangfan yiti*} defensive campaign {*fangyu zhanyi*} implemented against an air raiding enemy. The air defense campaign mainly includes campaign activities {*xingdong*} such as surface-to-air protection {*duikong fanghu*}, resistance operations {*kangji zuozhan*}, and counterattack operations {*fanji zuozhan*}. It is usually under unified command {*tongyi zhihui*} by a joint campaign commander [JCC] {*lianhe zhanyi zhihuiyuan*} and his command organ {*zhihui jiguan*}, and is conducted primarily by the Air Force, with the participation of related force-strengths {*bingli*} of the Army {*lujun*}, Navy, and Second Artillery Corps, and under complementation {*peihe*} by armed police units {*wujing budui*}, the militia {*minbing*}, and people's air defense strengths {*renmin fangkong liliang*}. The enemy in future air raids against us, in order to realize its air raid goals {*mudi*}, will rely on a powerful information warfare [IW] superiority {*xinxizhan youshi*}, to execute large-scale, high-intensity information attacks {*xinxi gongji*} against us. Our air defense operational strengths {*zuozhan liliang*} and important military and economic installations {*sheshi*} will be faced with serious electromagnetic [EM] threats.

The main missions of air defense campaign IO are as follows: to organize and implement IO reconnaissance {*zhencha*}, with the key points {*zhongdian*} on ascertaining the situation of the composition, deployment {*peizhi*}, and technical parameters {*canshu*} of the enemy's air raid operational reconnaissance and surveillance [R&S] systems {*zhencha jianshi xitong*}, command and control [C2] {*zhihui kongzhi*} systems, communication hubs {*tongxin shuniu*}, and air raid weaponry control {*kongxi bingqi kongzhi*} systems; to jam and sabotage {*ganrao, pohuai*} the enemy's air raid operational information systems and air raid weaponry control systems, so as to weaken the enemy air raid effects {*xiaoguo*} and to create favorable conditions for resistance operations; to jam and destroy {*cuihui*} the important targets in the enemy air defense operational information systems, so as to screen {*yanhu*} and assist-support {*zhiyuan*} the counterattack force-strengths in penetration {*tufang*} and assault {*strike*}; and to organize and implement information defense {*xinxi fangyu*}, so as to ensure operational information security [INFOSEC] {*xinxi anquan*} and the normal bringing into play of the information systems' operational effectiveness {*zuozhan xiaoneng*}. **[end of page 314]**

Section 1: Characteristics {*tedian*} of Air Defense Campaign IO…315

IO is an important component {*zucheng bufen*} of an air defense campaign. It often unfolds {*zhankai*} before the air defense campaign, and penetrates through the entire process of the air defense campaign, and has a major influence on the progress {*jincheng*} and outcome {*jieju*} of the air defense campaign. Air defense campaign IO possesses the following main characteristics.

I. The enemy air raid's targets of first choice are the critical nodes {*guanjian jiedian*} of our information systems, and the IW environment is sharp…315

Within air defense operations, the enemy air raid's targets of first choice will be the critical nodes of the adversary's information systems. By carrying out decisive strikes {*juedingxingde daji*} against information systems and critical nodes, [the enemy] will cause the adversary communication interrupts {*tongxin zhongduan*}, radar confusion and blindness {*leida mimang*}, command dysfunction {*zhihui shiling*}, and guided weapons going out of control {制导武器失控 *zhidao wuqi shikong*}, and thus will weaken and degrade the adversary's air defense operational capability {*zuozhan nengli*}. Our military, since its equipment {*zhuangbei*} technology is relatively backward, its intelligence early warning {*qingbao yujing*} means few, its reconnaissance facilities equipment {*zhencha shebei*} detection distance {*tance juli*} short, its intelligence processing automation degree low, and its early warning system's capability for resisting enemy jamming and destruction weak, will have great difficulty in timely grasping the enemy air raid intention {*qitu*}, and in ascertaining the enemy air raid's direction, scale, and targets. Added to this, the enemy attaches the greatest importance to the sustained quality {*chixuxing*} of air raid activities, and often continuously conducts them around the clock, not giving its adversary an opportunity to catch its breath. Hence, air defense campaign IO activities very likely will be caught off guard {猝不及防 *cubu jifang*}, even to the point where they unfold under circumstances of suffering the enemy's severe strikes. They will be faced with extremely sharp IW environments, and the campaign in its early phase very easily could fall into a passive position. The IO missions are thus extremely strenuous.

II. [IO] is faced with the enemy's integrated 3-dimensional [3-D] {*zonghe liti*} R&S and information attacks, and the position {*diwei*} of electronic air defense {*dianzi fangkong*} is prominent…315

In an air defense campaign, the various types of reconnaissance satellites {*gelei zhencha weixing*} which the enemy has dispositioned {*bushu*} in outer space {*taikong*} will be able every few hours to pass over our theater {*zhanqu shangkong*}, to conduct all-weather, uninterrupted {*bujianduan*} telemetry {*yaoce*} and surveillance. **[end of page 315]** [Enemy] strategic reconnaissance aerial vehicles {*zhanlue zhenchaji*}, early warning aircraft, and electronic warfare [EW] {*dianzizhan*} aircraft will be able at high altitudes over coastal areas {*yanhai diqu*} and even over international waters {*gonghai*} to conduct long-distance reconnaissance and early warning against our theater. Also, our theater campaign or tactical operations area {*zhanqu difu*} will be relatively narrow and small, the targets will be notably concentrated {*jizhong*}, and the campaign momentum disposition {*zhanyi bushi*} will have many points and broad areas {*dianduo mianguang*}. Our fixed radar, command communication {*zhihui tongxin*} systems, assembly zones {*jijie diyu*} and activities routes for massive forces groups {*zhongbing jituan*}, and large-scale equipment, in particular the bunkers {*yanti*} and cave depots {*dongku*} for "immovable" targets, will be exposed under the control of the enemy's "amplified" surveillance. At the same time, the enemy also will take electronic jamming {*dianzi*

ganrao} as the lead and stealth penetration {*yinshen tufang*} and stand-off precision strike {*fangquwai jingque daji*} as the main means, to carry out integrated strikes {*yitihua daji*}, with a mutual combination of joint fire strikes and information attacks, against our main war targets and information systems. Faced with intense information attacks, our air defense information systems may fall into paralysis {*tanhuan*}, so the position of "electronic air defense" will be prominent. Hence, this then requires that our military in terms of thought concepts {*sixiang guannian*} must establish the new concept of "electronic air defense," and realize the conversion from "firepower air defense" to "firepower air defense + electronic defense;" in terms of attack targets, realize the conversion from aerial platforms as primary to information systems as primary; and in terms of air defense means, realize the conversion from fire strike as primary to electronic attack {*dianzi gongji*} as primary. Electronic air defense not only includes applying EW means to conduct electronic jamming and sabotage against the air raiding enemy's information systems for early warning and detection and C2, and to paralyze the enemy's informationized air raid system of systems [SoS] {*xinxihua kongxi tixi*}, but also includes adopting means such as EM spectrum management and control {*dianci pinpu guankong*}, electronic camouflage {*dianzi weizhuang*}, and electronic deception {*dianzi qipian*}, to defend against enemy electronic reconnaissance {*dianzi zhencha*}. Electronic air defense has a multiplying {*beizeng*} and supplementary role {*buchong zuoyong*} vis-à-vis firepower air defense.

III. Operational strengths will have Air Force strengths in the lead, and air IO strengths will bring into play an important role…316

Within an air defense campaign, the side conducting an air raid mainly will use Air Force and Navy operational aircraft {*zuozhan feiji*} to conduct operational activities in the expansive airspace. Airborne reconnaissance {*kongzhong zhencha*} platforms such as airborne early warning aircraft {*kongzhong yujingji*}, electronic reconnaissance aircraft, and unmanned reconnaissance aerial vehicles [URAVs] {*wuren zhencha feiji*} will provide the air raid with intelligence assisting support {*qingbao zhiyuan*}, including reconnaissance, positioning {*dingwei*}, and strike effects evaluation appraisal {*daji xiaoguo pinggu*}. During the Kosovo War, NATO put into action aircraft flying a total of 37,000 sorties {*jiaci*} and executing air strikes over 78 days against the Federal Republic of Yugoslavia [FRY]; but never **[end of page 316]** did it step foot on FRY territory, and it concluded the war completely in the air. The side [implementing] air defense also inevitably will use the air as the main battlefield, because once the air raid's munitions {*danyao*} fall to the ground, the aftermath then cannot be changed. Faced with high-intensity, large-scope, long-range precision strike, [we] must attach importance to bringing into play the might {*weili*} of the air IO strengths. Compared to other IO means, air IO has distinct superiority, and its position within an air defense campaign is prominent. On one hand, [we] must jam and suppress {*ganrao, yazhi*} the electronic systems of the enemy's airborne early warning and command [AWACS] aircraft, reconnaissance aircraft, and outer space information assisting-support systems, to degrade the capability of the enemy reconnaissance for detecting targets and commanding and guiding {*zhihui yindao*} the air raid. On the other hand, [we] must conduct suppression of the airborne radar {*jizai leida*} and communication [systems] in

the enemy strike aircraft {*tuji feiji*} such as fighters {*jianjiji*} and bombers {*hongzhaji*}, to degrade the capability of aircraft penetration; and also must conduct jamming against the guidance equipment {*zhidao shebei*} of the enemy cruise missiles {*xunhang daodan*}, air-to-ground missiles [AGMs] {*kongduidi daodan*}, and precision guided bombs [GBUs] {*jingque zhidao zhadan*}, to degrade their hit accuracy {*mingzhong jingdu*}. All these activities take air and space {*kongtian*} as the main battlefield. To this end, [we] must construct an air fire distribution system {*kongzhong huoli peixi*} with a mutual combination of long, medium, and short {*yuan zhong di*} [ranges] and high, medium, and low altitudes {*gao zhong dikong*}, and even more must establish an electronic air defense operational SoS {*zuozhan tixi*} with a mutual combination of long-range communication jamming and early warning aircraft jamming, and with a mutual combination of precision guided munition [PGM] {*jingque zhidao wuqi*} jamming and jamming of enemy reconnaissance and early warning systems.

IV. Stealth technology {*yinshen jishu*} and full-dimensional protection {*quanwei fanghu*} thought will be applied on the battlefield, and the degree of difficulty in IO counterattack time opportunity {时机 *shiji*} selection is increased…317

Since the entry into the 1980s, stealth aircraft have been thrown into actual combat {*shizhan*}, and used for first attacks and first-batch penetration, destroying the defending side's surface-to-air warning and C2 {*duikong jingjie zhihui kongzhi*} and air defense firepower systems, and creating the conditions for operations by non-stealth aircraft. A stealth bomber's {*yinshen hongzhaji*} effective radar cross section [RCS] {*leida fanshe mianji*} is only equal to a few tenths of a percent down to 0.1% that of an old-style aircraft; and an active-service radar's detection distance {*faxian juli*} for it is extremely short or fundamentally nonexistent. Thus, this puts the use of radar as the main body for a surface-to-air warning net in dire straits, so that radar has lost its early warning function {*yujing gongneng*} for the air situation {*kongqing*}, and cannot support {*baozhang*} the air defense units {*fangkong budui*} in acquiring targets so they can throw themselves into combat.[15]

The enemy, while stressing the development of electronic defense technology, also has put forth the operational principle of "full-dimensional protection," which in each phase, each direction, and each level {*cengci*} of operations, **[end of page 317]** implements all-around protection {*quanmian baohu*} for friendly forces {*jifang budui*}. On the basis of possessing air dominance/supremacy {*zhikongquan*} over the operational space {*zuozhan kongjian*}, by providing force-strengths and installations with multilayer defensive tactics {*duoceng fangyu celue*}, this ensures that the enemy forces have freedom of activities {*xingdong ziyou*} in disposition and maneuver unfolding {*jidong*

[15] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

zhankai} and within the operational process. Full-dimensional protection tactical thought {*zhanshu sixiang*} can maximally boost the effects of air raid activities, and have increased the degree of difficulty in our air defense operations' selection of time opportunities for information counterattack operations.

V. EM attack and precision strike are the main operational means of the powerful enemy's air raids, and the IO strengths' protection and survival are faced with severe challenges…318

EM attack and precision strike already have become the main operational means for the enemy's execution of air raids, and this has constituted the maximum threat to all types of air defense weaponry and information targets in our theater. Several examples follow: high-performance electronic jamming aircraft can from several hundred kilometers away conduct intense jamming and suppression against electronic targets on tens of thousands of square kilometers of our air defense operations area (zone) {*zuozhan quyu*}. High-precision {*gaojingdu*} long-range guided weapons [can] execute beyond-visual-range [BVR] {*chaoshiju*} and stand-off firepower raids {*fangquwai huoli xiji*}. Using multiple means such as computer viruses {*jisuanji bingdu*} and network infiltration {*wangluo shentou*}, [the enemy] can sabotage the core facilities equipment of theater air defense campaign information systems and the critical installations for information weapons and equipment {*xinxi wuqi zhuangbei*}. [The enemy can] use EM pulse [EMP] weapons {*dianci maichong wuqi*} and special {*tezhong*} EW aircraft to suddenly launch strikes, putting our news media institutions into a paralyzed or semi-paralyzed state {*bantanhuan zhuangtai*}. [Finally,] adopting virtual reality [VR] {*xuni xianshi*} technology to switch signals {*qiehuan xinhao*} into our media facilities equipment, and using tendentious {*qingxiangxing*} voice, texts, and imagery to conduct reactionary political propaganda and psychological warfare [PSYWAR] {*xinlizhan*}, [the enemy] can shake our popular support and morale {*minxin shiqi*}, and influence social stability. At the same time, since the scale of our strengths and force-strengths {*liliang bingli*} participating in air defense campaign IO is limited, the jamming means are relatively unitary; [we] have a shortage/lack of GPS jamming strengths, anti-radiation {*fanfushe*} strengths, network attack {*wangluo gongji*} strengths, precision guided protection {精导防护 *jingdao fanghu*} strengths, and professional {*zhuanye*} electronic camouflage strengths. [Also,] battlefield information installations do not have full complements of equipment {*peitao*} and are not complete, the information system protection means are few, and the means for resisting enemy precision strike are limited. The entire information-strength operational strength SoS {*xinxi liliang zuozhan liliang tixi*} is faced with the double threat of "soft kill" {*"ruan shashang"*} and "hard destruction" {*"ying cuihui"*} by the enemy, so that the security protection and effective survival of IO systems are faced with severe challenges. **[end of page 318]**

Section 2: Requirements {*yaoqiu*} for Air Defense Campaign IO…319

Air defense campaign IO should firmly implement the strategic intent {*zhanlue yitu*} of "joint operations {*lianhe zuozhan*} and offensive air defense {*gongshi*

fangkong};" give full play to the integrated-whole might {*zhengti weili*} of omni-service and arm {*zhu junbingzhong*} IO; [achieve] unified command {*tongyi zhihui*}; have a rational momentum disposition; [effect] linkup of resistance, counterattack, and defense {抗, 反, 防衔接 *kang, fan, fang xianjie*}; take degrading of the enemy air raid information systems' effectiveness as the objective {*mubiao*}; take the electronic defense of important targets as the key point; take "integrated network and electronic" strikes [INEW] {*"wangdian yiti" daji*} as the main operational pattern {*zuozhan yangshi*}; and simultaneously use multiple means to seize and control information dominance in the battlefield's key point areas (zones) and critical time segments {*guanjian shijie*}.

I. Constructing a long-distance [long-range], large-scope, multilevel reconnaissance intelligence net {*zhencha qingbao wang*}, and doing all one can for early-stage early warning {*zaoqi yujing*}…319

The enemy will rely on its advanced command information system, to concentrate use of many types of standoff strike weapons, cruise missiles, new types of long-range guided cluster bombs {远程制导集束炸弹 *yuancheng zhidao jishu zhadan*}, joint standoff weapons [JSOWs] {*lianhe fangquwai wuqi*}, and joint direct attack munitions [JDAMs] {*lianhe zhijie gongji danyao*}, for key point strikes against the adversary air defense's close {*yanmi*} vital site targets {*yaohai mubiao*} and against fixed vital site targets in the strategic depth {*zhanlue zongshen*}. Only by establishing a comprehensive integrated {*zonghe yiti*} reconnaissance and early warning SoS can [we] from as far as possible detect incoming-raid targets, to provide accurate intelligence for the various types of air defense weapons, and to gain fairly long early warning time.

Early-stage early warning means that, according to the general disposition {*zongti bushu*} of the air defense campaign, and taking as support {*zhicheng*} the air channels {*kongzhong tongdao*} for the enemy's possible incoming raid and the air defense vital areas {*yaodi*} in our deep areas/belts {*zongshen didai*}, [we] as much as possible projectively deploy {*qianshen peizhi*} the theater IO strengths; increase the density of the set-up defense {*shefang midu*}; construct a long-distance, large-scope, multilevel reconnaissance intelligence early warning net; and conduct full-process monitoring {*quancheng jiankong*} of the enemy, to as early as possible detect the enemy air raid intention and signs {*zhenghou*}, and not lose a time opportunity to organize air defense operational activities. In concrete terms, this means [we] must in a unified manner organize the reconnaissance and early warning strengths of all services and arms within the theater scope, as well as the local satellite, aviation, navigation {*hanghai*}, and meteorology {*qixiang*} monitoring departments' {监测部门 *jiance bumen*} personnel and installations, **[end of page 319]** to constitute a "3-net, 1-center" {*"san wang yi zhongxin"*} early-stage early warning system with high- and low-[altitude] alternation {*gaodi jiaoti*}, with long and short [ranges] both covered {*yuanjin xiangqi*}, and with complementary functions {*gongneng hubu*}. First is the air situation reporting net {*kongqing baozhi wang*}. Composed of mainland radar, island and coast radar {*dao'an leida*}, airborne radar, and shipborne radar, its key points are on conducting monitoring of the Taiwan military's home islands {*taijun bendao*} and of the powerful enemy's

Asian-Pacific military bases {*jidi*}, as well as sea and air operational platforms, and from as far as possible detecting the enemy's incoming-raid targets. Second is the radio technique reconnaissance {*wuxiandian jishu zhencha*} and espionage {*diebao zhencha*} net. This is composed mainly of military/civilian-service {*jundi*} radio technique reconnaissance strengths and special reconnaissance {*tezhong zhencha*} strengths. It comprehensively applies {*zonghe yunyong*} various types of reconnaissance installations and means, to monitor {*zhenting*}, intercept {*jiehuo*}, position-find {*cewei*}, and analyze enemy radio information, and to timely grasp the situation of enemy air raid sorties {*kongxi chudong*}. Third is the surface-to-air observation/sentry net {*duikong guancha shaowang*}. The reconnaissance elements {*zhencha fendui*} of the various services and arms are composed mainly of the 1st-line units' subordinate reconnaissance elements, militia and reserve-duty professional elements {*minbing yubeiyi zhuanye fendui*}, and local people's air defense strengths. They use professional observation instrument equipment {*guancha qicai*} and expedient materials {*jiubian qicai*}; set up {*shezhi*} multipoint, multiline, multi-direction observation/sentry positions {*guanchashao zhendi*}; and carry out large-scope, uninterrupted air situation observation and reporting. Fourth is the air situation early-warning information processing center. It is composed of personnel transferred {*choudiao*} from various services and arms, as well as personnel from local related departments, and is set up within the joint command {*lianhe zhihuibu*}. This center mainly carries out rapid collection, screening {*zhenbie*}, and processing of enemy air raid information acquired by the various early warning networks, to provide a forceful basis for the JCC to set the resolution {*dingxia juexin*}.

II. Thoroughly organizing key point information protection, boosting the security and stability of the information systems…320

Within an air defense campaign, the JCC and his command organ must conduct thorough operations-research-based planning and organizing of IO protection activities, and adopt workable measures to resist the enemy's "soft kill," to withstand the enemy's "hard destruction," and to ensure the security and stability of information systems. First is rationally deploying and using electronic facilities equipment {*dianzi shebei*}. This means using full complements {*peitao*} of electronic equipment of different frequencies, different systems/formats {*tizhi*}, and different models {*xinghao*} to form a net, and bring into play the net's integrated-whole jam-resistance capability {*zhengti kangganrao nengli*}; [enforcing] strict EM spectrum management, and under the premise {*qianti*} of not influencing the fulfillment of campaign missions as much as possible reducing the number of start-ups {*kaiji*} and the operating time of the electronic equipment, and when necessary implementing radio silence {*wuxiandian jingmo*}; comprehensively applying multiple communication means, and as much as possible bringing into play **[end of page 320]** the role of underground wired electrical cables and fiberoptic communication {*guangxian tongxin*}; and properly controlling {*qiadang zhangwo*} the start-up timing {*qiyong shiji*} and quantity of concealed radar and backup communication facilities equipment {*beiyong tongxin shebei*} (channels {*xindao*}). Second is conducting electronic deception to confuse the enemy. This applies multiple electronic deception means to conceal the true and display the false {*yinzhen shijia*}, mix the spurious with

the genuine {以假乱真 *yijia luanzhen*}, and increase the enemy's difficulty in reconnaissance, jamming, and firepower destruction, so as to screen our electronic targets. Examples include using standard {制式 *zhishi*} or simple instrument equipment to simulate {*moni*} false wireless transceivers {*jia wuxian diantai*} and radar weaponry, applying technical instrument equipment in a false position {*jiazhendi*} to conduct virtual EM signal emissions {*xuni dianci xinhao fushe*}, irregularly {*wuguilyudi*} changing the radio signaling specifications {*wuxiandian lianluo guiding*}, and organizing electronic diversion/demonstration groupings {*dianzi yangdong qun*} to simulate the transceiver net {*diantai wang*} of our air defense operational command center. Third is [implementing] a mutual combination of "hiding" {"藏" *"cang"*} and "avoiding" {"避" *"bi"*}. Communication, navigation {*daohang*}, radar, and similar electronic facilities equipment, on the basis of decentralized and hidden deployment {*fensan, yinbi peizhi*}, [should] exploit a variety of technical means and fully exploit the terrain and surface features {*diwu*} to carry out counter-radar, counter-infrared [counter-IR], and counter-electro-optical [counter-EO] {*fanguangdian*} reconnaissance camouflage, to cause the enemy difficulty in detection and identification. When electrical facilities equipment encounters jamming, [the JCC and command organ should] swiftly change the signal parameters or employ directional antennas to evade the enemy's electronic jamming. [They should] exploit operational intervals to timely move positions {*zhuanyi zhendi*}, so as to avoid the enemy's jamming and suppression and strikes. Fourth is establishing passive detection {*wuyuan tance*} systems. In our backbone radar and ground air defense weapons positions, they deploy passive detection (electronic reconnaissance, IR reconnaissance, etc.) facilities equipment; and in forward areas {*qianyan diqu*} and in deep areas in the enemy's main incoming-raid direction, they establish independent passive reconnaissance posts {*wuyuan zhencha zhan*}, build a passive detection system, and coordinate {*xietong*} work with the air defense radar, to jointly fulfill the surface-to-air reconnaissance mission.

III. Attaching importance to jamming of the enemy's space-based {*tianji*} information systems, and blocking and severing {*zuse geduan*} their contacts to the ground, sea surface, and air…321

Within an air defense campaign, in the important ground mark areas (zones) {地标区域 *dibiao quyu*}, [the JCC and command organ should] exploit multiple electronic jammers {*dianzi ganraoji*}, adopting surface-to-air mode {*diduikong fangshi*}, to approximately vertically transmit jamming waves {*ganrao dianbo*} into the air, and form a jamming wall {*ganrao qiang*}. This can effectively sever and block the space-based information systems which provide reconnaissance intelligence, positioning and navigation {*dingwei daohang*}, and signal communication {*tongxin lianluo*} support to the air raid weaponry, so that it cannot normally receive ground-to-space and space-to-ground signals {*diduitian he tianduidi xinhao*}. During the Persian Gulf War {*haiwan zhanzheng*} and Iraq War, more than 85% of the US military's long-distance communication relied on defense satellite communication systems dispositioned in outer space. **[end of page 321]** The mid-course guidance {*zhongduan zhidao*} of cruise missiles and other long-distance air-to-ground attack missiles [AGMs] {*kongdi gongji*

daodan}, and the flight navigation {*feixing daohang*} of operational aircraft including stealth aircraft, as well as the plotting {*biaohui*} of land and sea mine fields {*leichang*}, and even determining {*ceding*} of the location of downed flying personnel {*feixing renyuan*}, all mainly rely on navigation satellite [navsat] timing and range-finding {计时与测距 *jishi yu ceju*} systems (the global positioning system [GPS] {*quanqiu dingwei xitong*}). Thus, within an air defense campaign, [the JCC and command organ] should attach importance to conducting jamming and suppression of the enemy's space-based information systems dispositioned in outer space, or use hard-kill weapons {*ying shashang wuqi*} to destroy them, so as to sever their contacts to the ground and sea surface, [and thus] indirectly but effectively assist-support the air defense resistance operations.

IV. Taking the enemy incoming-raid main direction as the key point, establishing an IO disposition which has attack and defense integrated {*gongfang yiti*}, with attack as primary…322

An air defense campaign should rely on the theater's forward edge {*zhanqu qianyan*} and facing sea zone {*dangmian haiyu*}; forward-deploy force-strengths and weapons {*qianzhi bingli bingqi*}; establish an operational disposition which takes containing and controlling {扼控 *ekong*} the enemy's main incoming-raid direction as the key point, which has a combination of points and lines {*dianxian jiehe*} and a combination of statics and dynamics {*dongjing jiehe*}, and which has attack and defense integrated, with attack as primary; and [thus] execute effective strikes against the enemy. First is exploiting the facing sea zone for a projective disposition {*qianshen bushu*}, and establishing a reconnaissance and early warning area. Second is focusing on the enemy's main incoming-raid direction for an echelon disposition {*tici bushu*}, and establishing a 3-D, multipath electronic jamming belt {*dianzi ganrao dai*}. Third is giving consideration also to the enemy incoming raid's flank directions {*yice fangxiang*} for a mobile disposition {*jidong bushu*}, and establishing mobile electronic jamming positions. Fourth is centering on the important targets for a circular disposition {*huanxing bushu*}, and establishing an area (zone) electronic protection belt {*dianzi fanghu dai*}. When the enemy air raid weaponry enters the jamming scope, [we] conduct comprehensive jamming of the enemy, to degrade the enemy information systems' effectiveness, to complement the first strike activities, and to protect the security of important targets.

V. Focusing on sabotaging the structure of the enemy's air raid information systems, and executing effective information attacks {*xinxi jingong*}…322

The air raid operational system is a comprehensive operational system composed of all services and arms. Its organization is extremely rigorous {*yanmi*}, and within it, if one subsystem {*zixitong*} encounters sabotage, this will cause the entire operational system's effectiveness to sharply degrade, and even to lose its operational capability. Air raid operations especially emphasize the command and guidance {*zhihui yindao*} role of the early warning and C2 systems, and the complementary screening {*peihe yanhu*} role of electronic jamming systems. Hence, focusing on the characteristics of air raid activities

which take information systems as the link {*niudai*} and support {*zhicheng*}, **[end of page 322]** [the JCC and command organ] select these information systems' communication channels and critical nodes as the targets; concentrate the information strengths to form strike "fists;" and, under complementation by means such as integrated firepower destruction {*zonghe huoli cuihui*}, PGM strikes, and special operations forces sabotage-raids {*tezhong zuozhan liliang poxi*}, inflict heavy losses {*zhongchuang*} on the enemy, and strive to "attack its vital sites, to damage the entire body" {"点其要害, 伤其全身" *"dianqi yaohai, shangqi quanshen"*}. To this end, they should in advance {*yuxian*} deploy the air defense campaign IO strengths into a campaign momentum disposition {*zhanyi bushi*} favorable to meeting the enemy; rigorously control the enemy's various types of air raid information; and in case of needs and requirements {*xuyao*}, immediately launch surprise, fierce, continuous information attacks {*xinxi gongji*} against the enemy, to firmly seize the campaign initiative {*zhudongquan*}. First is [seizing] the first opportunity to attack {*xianji gongji*}. [They should] concentrate elite troops and efficient instruments {*jingbing liqi*}, seize a favorable time opportunity, resolutely launch the attack, and do all they can to see that the enemy air raid weaponry is blocked at the time of takeoff {*chudong*}, harassed during flight, and destroyed before it bombs {*baozha*} [us]. Second is attacking the enemy air raid operational command system. At or before the air defense campaign's launch, they concentrate the IO strengths of the units and of the local area, to execute high-intensity intensive EM surprise attacks {*miji dianci tuxi*} against the command system for the enemy air raid operational platforms, to cause the enemy's local information systems to be damaged or seriously blocked. Third is attacking the enemy's intelligence early warning system. In already set-up operations areas (zones) and in the direction of the enemy incoming air raid, they set up "EM shielding areas" {*"dianci pingbi qu"*} and "jamming corridors" {*"ganrao zoulang"*}, and conduct powerful jamming and suppression against the enemy, to sever the enemy early warning information chain. Fourth is attacking the enemy communication system. [Special forces] adopt various forms {*xingshi*} to penetrate far behind enemy lines {*shenru dihou*}, and sabotage the enemy communication channels and communication relay {*tongxin jieli*} installations, so that the enemy loses its basic information backing {*yituo*}, and thus finds itself in dire straits.

Section 3: Air Defense Campaign IO Activities…323

Air defense campaign IO activities should tightly center on the unfolding of the resistance operations, counterattack operations, and protection activities; focus on the characteristics and requirements of the air defense campaign; flexibly {*linghuo*} adopt a variety of IO methods and means; and do all they can to gain the optimal IO effects. **[end of page 323]**

I. IO activities during protection…324

The JCC and his campaign organ should comprehensively apply various types of IO strengths. The key points are on organizing counter-enemy information reconnaissance {*fandi xinxi zhencha*}, jamming and deception of enemy air raid

weaponry control systems, degrading the enemy air raid's effects, and assisting-supporting and complementing the other operational strengths in protecting the security of important targets.

Organizing counter-enemy information reconnaissance: [the JCC] should command all operational groups (groupings) {*zuozhan jituan (qun)*} to focus on the enemy high-tech reconnaissance means {*zhencha shouduan*} and their application modes, and exploit various technical means to implement counter-radar and counter-EO reconnaissance camouflage for the protection targets; conduct electronic diversion/demonstration, and exploit standard and simple instrument equipment to set up false targets {*jiamubiao*} and false positions and to simulate false radiation sources {*jiafushe yuan*}, so as to deceive and confuse the enemy; strictly manage the EM spectrum and control EM radiation {*dianci fushe*}; and in good time organize soft- and hard-kill {*ruanying shashang*} strengths, to jam and destroy the enemy's reconnaissance systems and degrade the enemy's information reconnaissance effects.

Organizing defense against enemy precision strike: [the JCC] should command all operational groups (groupings) to use navigation positioning {*daohang dingwei*} jamming facilities equipment to jam the satellite navigation positioning systems of the enemy air raid weaponry; exploit electronic camouflage instrument equipment, to alter the EM traits {*texing*} of the targets and target areas; in the skies over the target areas, project chaff {*ganrao botiao*}, release smoke and water vapor or spray aerosols {*qirongjiao*}, to attenuate the targets' EO radiated (reflected) signal or to block laser beams {*jiguang shu*}; in the vicinity of the protection targets, deploy EO deception jammers {*guangdian qipian ganraoji*} or decoys {*youer*}, to lure the enemy guided weapons away from the targets; use laser or microwave weapons {*weibo wuqi*} to blind and jam the enemy guided weapons' EO sensors {*guangdian chuanganqi*} or to intercept {*lanjie*} the enemy guided weapons; and employ ground-to-air {*diduikong*} jamming strengths, to jam and suppress the enemy airborne aiming radar {*jizai miaozhun leida*}, missile guidance {*daodan zhidao*} systems, and fire control radar {*huokong leida*} and radio/wireless communication {*wuxiandian tongxin*}, to weaken to the maximum extent the strike effects of the enemy air raid weaponry.

II. IO during resistance operations…324

The JCC and his command organ should place the key points on organizing information systems protection and information attack activities, and on assisting-supporting and complementing the resistance operational activities of the other operational strengths. **[end of page 324]**

When the enemy executes an information attack, they should organize and command all operational groups (groupings) to comprehensively apply multiple means and measures, including concealment and camouflage {*yinbi weizhuang*}, engineering protection, control of EM radiation, decoys and deception, maneuver and evasion {*jidong guibi*}, and force-strength and firepower screening, to carry out protection of important

information system targets within the air defense SoS, and defend against the enemy's anti-radiation weapons and other firepower destruction; comprehensively apply technical, tactical, and management measures to counter enemy electronic jamming and defend against enemy network attacks; per their approved authority limits {*quanxian*}, at the right time start using hidden frequencies {*yinbi pinlyu*} and channels; organize air and surface-to-air fire strikes at enemy EW aircraft, to intercept {*jieji*} the enemy anti-radiation weapons and wipe out {*xiaomie*} the threat sources; and for information systems which have suffered enemy sabotage, they should timely ascertain the damage situation, and adopt effective measures to rapidly recover information system functions.

When conducting resistance operations, [the JCC and command organ] should concentrate the use of air and ground (sea) electronic jamming strengths, to conduct jamming of air and sea early warning and C2 systems and airborne (shipborne) {*ji (jian) zai*} communication and navigation facilities equipment in the enemy direction of main attack {*zhugong fangxiang*}; comprehensively apply anti-radiation weapons and other firepower, to strike at the enemy's airborne early warning aircraft, EW aircraft, and ground (sea) early warning and detection and EW systems; use aviation {*hangkong*} jamming strengths to jam the enemy airborne fire control radar and to screen interceptor aircraft {*lanjie feiji*} in concealed closing with the enemy {*jiedi*} and executing attacks before the enemy can; use network attack means to execute attacks against enemy network systems and facilities equipment; and employ satellite countermeasures {*weixing duikang*} systems and special IW weapons {*tezhong xinxizhan wuqi*} to jam, blind, or destroy the enemy space {*kongjian*} information systems, weaken the enemy air raid operational effects, and assist-support and complement the resistance operational activities of all operational groups (groupings).

III. IO during counterattack operations…325

The JCC and his command organ should organize and command the IO groups (task groups {*jiqun*}) to comprehensively apply various information attack strengths, under complementation by other strengths, to execute jamming and destruction of the enemy information system's vital site targets, so as to assist-support and screen the counterattack force-strengths' penetration {*tufang*} and assault {*tuji*}.

At the start of or slightly before the counterattack activities, in the direction of diversion {*yangdong*} or diversionary attack {*yanggong*}, with electronic jamming **[end of page 325]** and diversion as primary, [the JCC and command organ should] comprehensively apply multiple electronic deception means to complement force-strength diversion or firepower diversionary attack, to decentralize {*fensan*} the enemy's attention, to move {*diaodong*} and contain {*qianzhi*} the enemy resistance force-strengths, and to form a battlefield posture {*taishi*} favorable to counterattack activities. When executing missile firepower strikes against the enemy, they should comprehensively apply means such as airborne, shipborne, and missile-mounted {机, 舰, 弹载 *ji, jian, danzai*} electronic jamming facilities equipment, anti-radiation weapons, and ground high-power jamming systems, as well as false payloads {*jiadantou*}, to

conduct jamming, destruction, or deception of enemy anti-missile {*fandao*} systems, so as to screen missile penetration. When executing aviation forces {*hangkongbing*} counterattack, in the strike direction, they should comprehensively apply air, ground, and sea jamming strengths, as well as anti-radiation weapons, to jam and attack the enemy airborne early warning aircraft, ground (shipborne) air defense radar, air defense C2 systems, interceptor aircraft, and surface-to-air weapon fire control systems, so as to complement the airborne suppression formations {*kongzhong yazhi biandui*}, screen the formations in opening up penetration corridors {*tufang zoulang*}, and support the strike formations in penetration and strikes. After strikes against predetermined targets, using electronic jamming means as primary, they [should] screen the aviation forces' return flight.

Before or during the process of the counterattack operations, they should apply network attack strengths to execute attacks against the network systems of the enemy air defense SoS, and do all they can to paralyze the enemy air defense SoS and weaken the enemy resistance capability; organize psychological attack {*xinli gongji*} strengths in applying means such as public opinion {*yulun*} propaganda and PSYWAR weapons, to execute psychological attacks against the enemy, so as to split up and disintegrate {*fenhua wajie*} the hostile forces {敌对势力 *didui shili*}, shake the enemy troops' morale {*junxin*}, arouse enemy anti-war sentiment {*fanzhan qingxu*}, and assist-support and complement the air defense operational activities of the other operational strengths. At the same time, they should strengthen IO reconnaissance and information defense, to support the smooth conduct of the counterattack operations. **[end of page 326; end of chapter]**

This page intentionally left blank.

Chapter 20
Joint Campaign Information Operations Effectiveness Evaluation…327

The joint campaign information operations [IO] effectiveness evaluation is an appraisal and estimate conducted for operational results generated from IO activities within a joint campaign, and its goal is for the joint campaign IO commander and his command organ to scientifically organize {*kexue zuzhi*} the operations research-based planning {*chouhua*} of joint campaign IO. The joint campaign IO effectiveness evaluation is an indispensable content within the course of joint campaign IO and it has an important significance for improving joint campaign IO decision-making quality and IO capabilities.

Section 1: Principles of Joint Campaign IO Effectiveness Evaluation…327

The principles of joint campaign IO effectiveness evaluation refer to the rules and standards {*faze*} that must be adhered to within IO effectiveness evaluation in a joint campaign, and regarding accurately and scientifically conducting joint campaign IO evaluations, the correct determination of effectiveness evaluation theory has important guidance significance. To evaluate joint campaign IO effectiveness, one should start out from the needs of joint campaign IO command and abide by the following principles.[16]
[End of page 327]

I. Quantitative in the lead, and supplemented by qualitative…328

[The principle of] Quantitative in the lead and supplemented by qualitative refers to when combining the means of quantitative evaluation with qualitative evaluation during the course of joint campaign IO effectiveness evaluations, the main means is quantitative evaluation supplemented by qualitative evaluation to obtain a quantified result. Conducting a complete and comprehensive qualitative evaluation for joint campaign IO effectiveness is the basis for quantitative evaluation, and this ensures that quantified processing is conducted for each effectiveness factor possesses a scientific quality. The results of quantitative evaluations also push forward the improvements in the quality of qualitative evaluations. For example, the indices factors such as electronic equipment reconnaissance capability, attack capability, defense capability, network reconnaissance capability, attack capability, defensive capability all can be relied on for determining tactical and technical parameters, and through data collection during the course of operations, various effective data are plentiful and quantitative evaluation means will adopt and even occupy a dominant position. Moreover, qualitative and quantitative evaluations are both complementary and complete within effectiveness

[16] Xu Xiaoyan: *Science of Information Operations*, PLA Press, 2002, p. 487.

evaluations – only stressing quantitative analysis places evaluation results into long-standing mistaken ideas of unstable foundations and only paying attention to qualitative analysis cause evaluations to lose their usability. We should adhere to the usability and accuracy of joint IO effectiveness evaluation results and establish a foothold in quantitative evaluation while aided by qualitative evaluation to obtain scientifically quantified results.

II. Integrated-whole analysis, synthesized evaluations…328

Integrated-whole analysis {*zhengti fenxi*} and synthesized evaluations {*zonghe pinggu*} refers to conducting a complete and thorough analysis for joint campaign IO effectiveness and giving prominence to the integrated-whole quality and synthesized quality of effectiveness evaluations to obtain evaluation results. There are many factors that reflect joint campaign IO effectiveness, and every factor is only one facet of operational effectiveness so only by conducting a synthesized evaluation of the evaluation results in every aspect can obtain scientific evaluation conclusions. The joint campaign IO effectiveness evaluation is a synthesized evaluation of operational effects such as electronic warfare, computer network warfare, psychological warfare, etc. within a joint campaign. They are also but one domain within joint campaign IO, if only considering one by itself or separately, one cannot form an integrated-whole **[end of page 328]** and will only obtain a partial conclusion. Thereby, when conducting an evaluation of joint campaign IO effectiveness, one must persist in the principle of integrated-whole analysis and synthesized evaluation.

III. Give prominence to vital points, and be rational in controlling…329

Giving prominence to vital points {*yaodian tuchu*} and being rational in controlling {约束合理 *yueshu heli*} refers to selecting rational control conditions when conducting joint campaign IO effectiveness evaluations and to conducting evaluations by given prominence to vital point issues. There are many factors touched upon in joint campaign IO effectiveness evaluations, for example, personnel quality, unit training levels, natural environment, technical environment, enemy information, our information, and friendly information, etc., of these factors, some have decisive quality role in joint campaign IO effectiveness, and some factors have a very small effectiveness influence on operations. One must pay attention in grasping the main contradictions and separating the main from the secondary amongst these influencing factors. For example, conduct vital point analysis areas that have a critical role for joint campaign IO effectiveness such as command and control systems, communications and electronic systems, computer systems, reconnaissance systems, surveillance systems, enemy information and our information, and only conduct necessary analysis as supplemental for secondary factors such as personnel and environment so as to avoid expending too much effort in non-essential problems. Joint campaign IO effectiveness evaluations are conducted under specific operational backdrops and without rational control conditions, the conducted evaluations not only have no practical sense but their evaluation results will not be accurate.

IV. Scientifically establish the model, and flexibly apply the method…329

Scientifically establish the model and flexibly apply the method refers to establishing a scientific evaluation model prior to conducting joint campaign IO effectiveness evaluations, and based on evaluation objectives, flexibly select different evaluation methods. Establishing the evaluation model is an important means of joint campaign IO effectiveness and a scientific establishment of the model benefits the evaluator to put in good order his train of thinking and gain clarity for the critical links; it also benefits the commander in comprehending the guidance significance of the joint campaign IO effectiveness evaluation through modeling. After the joint campaign IO effectiveness evaluation model is established, one must, based on the differences in evaluation objectives, **[end of page 329]** flexibly select different evaluation methods to resolve the problems encountered during the evaluation course. For evaluation objectives and evaluation indices having cause-effect relationships, adopt the analytic method {*jiexi fa*}. For example, for reliability of joint campaign information systems, one can use analysis such as the mean failure rate {*pingjun guzhanglyu*}, average failure time {*pingjun guzhang shijian*}, mean time between failure {*pingjun guzhang shijian*}, etc.; for selecting operational courses of action {*zuozhan fang'an*}, due to the large variability in operational activities, one can use the computer simulation method to conduct optimizations.

Section 2: Main Methods of Joint Campaign IO Effectiveness Evaluation…330

Joint campaign IO effectiveness evaluation methods have many interlinking parts with ordinary methods of systems analysis, but they also have their own special qualities. For joint campaign IO effectiveness evaluation methods, there is mainly the multi-attribute utility analysis method, fuzzy synthetic evaluation method, grey correlation evaluation method, computer simulation method, and live force exercise and training evaluation method.

I. Multi-attribute utility analysis method…330

The multi-attribute utility analysis method[17] is, in the joint campaign IO effectiveness evaluation, whereby one combines the many indices and a variety of evaluation conditions to solve a complex problem of synthetic evaluation. It has much superiority over the utility method in single objective decision-making analysis, which is to say that one can smoothly solve a complex evaluation problem caused by combining multiple indices and a variety of evaluation conditions in evaluating joint campaign IO

[17] Guo Qisheng {郭齐胜}, et al. Introduction to Equipment Effectiveness Evaluations {zhuangbei xiaoneng pinggu gailun}, Defense Industries Press, 2005, p. 83.

effectiveness. However, what must be pointed out is, due to multi-attribute utility analysis being a method needing-requiring the utility function, it does not have a unique quality. Therefore, when evaluating joint campaign IO effectiveness, it is closely related to the special love of the decision-maker or decision-making style, and thus while the solution created from the problem is also not **[end of page 330]** unique, it similarly depends upon the special love of the decision-maker or the decision-making style. Consequently, the crux and the point of difficulty of applying multi-attribute utility analysis method in evaluating joint campaign IO effectiveness for the most part lies in determining multi-attribute utility functions.

II. Fuzzy synthetic evaluation method…331

The fuzzy synthetic evaluation method,[18] on the basis of fuzzy mathematics, applies the tenet of combining fuzzy relationships, and for the things and objects restricted by a variety of factors, it quantifies some factors that are not clear or not easy to quantify; based on the fuzzy criteria and parameters of multiple items, it conducts a synthetic judgment {*zonghe pingpan*} of alternative courses of action {*beixuan fang'an*}, and furthermore, in accordance with the results of synthetic judgment, it conducts a comparative sorting of each alternative course of action, thus it's a method for selecting a best course of action.

For evaluation of joint campaign IO effectiveness, there are many factors to consider, not only must it consider the inherent capability of the joint campaign IO system itself, but it also must consider the effects of factors such as battlefield environment, human environment and technical environment have on bringing into play its [system's] operational effectiveness. Also, in terms of live force exercise and training, simulation testing and on the battlefield, because it is very difficult to use a definitive value to express this, one can only conduct research via the aid of a fuzzy notion. Moreover, it is very difficult to obtain an accurate value for depicting a soft strike against the enemy in joint campaign IO, this is a fuzzy notion. Therefore, using fuzzy theory to conduct evaluations of joint campaign IO effectiveness both conforms to reality and is necessary.

III. Grey correlation evaluation method…331

The grey correlation evaluation method[19] {*huise guanlian pinggu fa*} is a multi-factor statistical analysis method. With a sample data of each factor as basis, it uses grey

[18] Guo Qisheng, et al: Introduction to Equipment Effectiveness Evaluations {zhuangbei xiaoneng pinggu gailun}, Defense Industries Press, 2005, p. 87.

[19] Liu Sifeng {刘思峰}, et al. Grey System Theory and Its Applications {huise xitong lilun ji qi yingyong}, Science Press 2004, p. 40.

correlation level to depict the relational strengths or weaknesses between factors **[end of page 331]**, their sizes and order-sequence; it mainly analyzes the correlative size between various component factors and the integrated-whole. The object of its manipulation is the time sequence of each factor, and for multiple indices synthetic evaluation objects, one can view the comparative sequence as a sequence constructed from each index value of the thing being evaluated. Its reference sequence is an ideal comparative index, and given the revelations of distance evaluation {*juli pinggu*}, one selects the optimum index data and worst index data as the reference data series {*cankao shulie*}, compares the correlation levels between each operational course of action's optimum and worst courses of action, and evaluates the superiority or inferiority of the various courses of action.

IV. Computer simulation method…332

The computer simulation method is a method for conducting analytical evaluation undergone by establishing mathematical modeling and electronic computer laboratory as the basis, studying the quantitative relationships in joint campaign IO activities and conducting an analytical evaluation of the joint campaign IO effectiveness. It brings to light the quantitative change process {*liangbian guocheng*} of IO activities, it discovers the boundaries from quantitative change to qualitative change and it is complementary and complete with qualitative research. One can, through computer simulation of the joint campaign operations environment, forecast the results of joint campaign IO approaches {*celue*} and plans, evaluate effectiveness of IO weapon systems, stimulate new operational thought and it is an important means for evaluating joint campaign IO effectiveness.

The computer simulation method is an appraisal made under a condition of confrontation and with the backdrop of a specific operational environment and a specific force strength task-organization; it can implement a demonstration of a combat process, and though is fairly visual, it requires a large amount of reliable foundation data and original source material as basis. Computer simulation reflects the confrontation conditions and the object of engagement to a specific degree; it considers the role of weapons and equipment coordination, and all of the operational effectiveness attributes of weapons and equipment systems manifested in the full course of operations and the differences of different scale operational effectiveness particularly conform to this forecasting evaluation of conducting joint campaign IO weapon systems or operational courses of action.

V. Live force exercise and training evaluation method…332

The live force exercise evaluation method refers to, through a joint campaign IO exercise and training **[end of page 332]** and during operational exercises and training, conducting analytical evaluation and forecasting of content such as the joint campaign IO combat director's {*zhizhanyuan*} capabilities of applying IO weapons and equipment and operational courses of action, etc. The live force exercise and training evaluation method

possesses a repetitive quality, and the conclusion of effectiveness analysis evaluation is affected by the life-like level of the exercise and training.

When implementing live force exercise and training, one must pay attention in seizing upon three links {*huanjie*}: first is establishing a scientific live force exercise and training evaluation department. Joint campaign IO touches upon a broad spectrum of services and arms, and its technical content is higher while its evaluation work is extremely complex. Therefore, the personnel participating in live force exercise and training evaluations should include personnel such as the unit's senior officers' organ, military experts and technical experts and they must possess higher accomplishments and experiences in areas such as joint campaigns and IO. Second is establishing rational live force exercise and training evaluation content. For evaluation content, one should design exercise and training topics based on future joint campaign operational missions, centering on the topic to determine the live force exercise and training content, and based on this content, determine evaluation scope and content. Third is formulating objective live force exercise and training achievement assessment standards {实兵演练成绩评定标准 *shibing yanlian chengji pingding biaozhun*}. In order to allow live force exercise and training to have standards and the evaluations have a basis, one must establish live force exercise and training achievement assessment standards.

Section 3: The Joint Campaign IO Effectiveness Evaluation Index *tixi* System…333

For evaluation of joint campaign IO effectiveness, one must formulate an ample and robust index *tixi* system that manifests the characteristics of joint campaign IO before one can conduct a complete and objective analysis of joint campaign IO effectiveness. In this manner, one can fundamentally ensure the scientific quality of the evaluation, prevent tremendous disparity created from differences in evaluator knowledge and capabilities, and overcome the practice of solely relying on sweeping evaluations from subjective impressions. The joint campaign IO effectiveness evaluation index *tixi* system can normally be divided into the IO reconnaissance capabilities, information attack capabilities, information defense capabilities, and information support capabilities. **[End of page 333]**

I. Information reconnaissance capabilities…334

Information reconnaissance capabilities are constituted from the following types of capabilities.

(1) Electronic reconnaissance capability

Electronic reconnaissance capability mainly includes ground, air, sea and satellite early warning capabilities. Ordinarily, the electronic reconnaissance capability's specific indices are: reconnaissance sustained times, reconnaissance early warning range, reconnaissance sensitivity, number of same time reconnaissance targets, etc.

(2) Network reconnaissance capability

Network reconnaissance capability mainly includes the capabilities in aspects such as leak scanning {*loudong saomiao*}, acquisition of orders {*haoling huoqu*}, and code-breaking. Ordinarily, network reconnaissance capability's specific indices are: probability of network scanner detecting leaks, probability of acquiring orders, probability of breaking codes, and network reconnaissance response time, etc.

(3) Special reconnaissance capability

Special reconnaissance capability mainly touches upon unit quality and equipment and instruments, etc.

II. Information attack capabilities…334

Information attack capabilities are mainly constituted from the following types of capabilities.

(1) Electronic jamming capability

Electronic jamming capability mainly includes: implementing communications jamming against the enemy, radar jamming, electro-optical jamming, jamming against sonars, and navigational jamming capabilities. Ordinarily, its indices are: jamming power, jamming range, jamming frequency bands, jamming response time, jamming targets, etc.

(2) Network attack capability

Network attack capability mainly includes: virus insertion and hacker attacks. The main indices are: probability of penetrating the network, probability of safely withdrawing without detection, information data disruption degree, attack response time, etc. **[End of page 334]**

(3) Psychological warfare capability

Psychological warfare capability mainly includes: capability for implementing psychological promulgation, psychological deception {*xinli qizha*}, and psychological deterrence against the enemy's command officers, units and communications media.

(4) Physical destruct capability

Physical destruct capability mainly includes: destruction capability for applying precision guidance weapons against information systems, strike capability of anti-radiation weapons and directed energy weapons against electronic equipment, as well as

the disruption capability of special operations units against critical parts such as information nodes, etc. Ordinarily, the indices are: probability of discovering targets and the degree of damage.

III. Information defense capabilities…335

Information defense capabilities are mainly constituted of the following types of capabilities.

(1) Electronic counter-jamming capability

Electronic counter-jamming capability mainly includes: radar counter-jamming, electro-optical counter-jamming and communications counter-jamming capabilities. The indices of counter-jamming capability are mainly manifested in the *tizhi* system of time selection quality, space selection quality, frequency selection quality, power selection quality.

(2) Network protection capability

Network protection capability mainly includes: access control capability {*fangwen kongzhi nengli*}, system security capability, secure network management capability, utility service capability {*shiyong fuwu nengli*}, etc. Access control touches upon order control {*kouling kongzhi*}, identification authentication and access rights. System security touches upon network protection, information encryption. Secure network management touches upon network management security, secure key management and integrated security networks. Utility service touches upon denial of service {*fang jujue fuwu*} and secure applications {*anquan yingyong*}.

(3) Counter-psychological warfare capability

Counter-psychological warfare capability mainly includes: capability to counter the enemy's implementation of psychological propaganda, psychological deception and psychological deterrence.

(4) Anti-destruct capability of information systems

The anti-destruct capabilities of information systems mainly include maintenance capability, concealment and camouflage capability, **[end of page 335]** and maneuver capability, etc. Maintenance capability can use indices such as mean time of repair, and degree of repair, etc. Concealment and camouflage capability touches upon the strength of protection against magnetic leaks {*fangci xielou de qiangdu*} and engineering protection. Ordinarily, for maneuver capability, one can use speed to evaluate.

IV. Information support capabilities…336

Information support capabilities are mainly constituted from the following types of capabilities.

(1) Information processing and control capabilities

Ordinarily, the indices of information processing and control capabilities are: intelligence synthesis ratio {*qingbao zonghe bi*}: the ratio between the synthesized intelligence volume generated after system processing {*xitong jiagong*} and the raw intelligence volume {*yuanshi qingbao liang*} input into the system {*shuru xitong*} – it reflects the synthesis capability of the system for raw intelligence; information processing density {*xinxi chuli midu*}: total volume of information processed by the system within a single unit of time; information storage volume: total amount of information the system can store; resource utilization rate {*ziyuang liyong lyu*}: ratio of resource capacity being used and the system's total resource capacity; quality of information processing: conformance level between information processed results and the results of usage requirements, including precision of information processing, confidence and utility of processed results, etc.; as well as precision and self-adaptability of system controls, etc.

(2) Information dissemination capability

Ordinarily, the indices of information dissemination capability are: throughput {吞吐量 *tuntuliang*}, transmission time lag {传输时延 *chuanshu shiyan*}, connectivity rate {连通率 *liantong lyu*} and bit error rate {误码率 *wuma lyu*}.

(3) Equipment and instruments and technical support capability

Ordinarily, equipment and instruments and technical support capability are: real-time quality, reliability, and supportability, etc.

(4) Equipment maintenance and supply capability

Equipment maintenance and supply capability is mainly manifested in: equipment maintenance speed, equipment maintenance categories, equipment maintenance quality, equipment inventory {*zhuangbei kucunliang*}, equipment inventory categories, inventory equipment quality, and equipment transport capability. **[End of page 336]**

(5) Personnel recovery and supply capability

Personnel recovery and supply capability {*renyuan huifu yu buji nengli*} is mainly manifested in: living support capability {*shenghuo baozhang nengli*}, battlefield rescue capability, personnel that can be supplied amount, supplied personnel quality, personnel transport capability.

Section 4: Implementation Steps of Joint Campaign IO Effectiveness Evaluation…337

Joint campaign IO effectiveness evaluation is complex work so one should, relying on the relevant principles, flexibly select the evaluation method, scientifically organize and implement, and synthesize the analysis evaluation conclusion. The implementation methods of joint campaign IO effectiveness evaluation are normally divided into three steps of determining evaluation method, organizing and implementing, and analyzing and utilizing the effectiveness evaluation conclusion.

I. Determining the evaluation method…337

When evaluating joint campaign IO effectiveness, one should first, in accordance with the evaluation needs and evaluation objectives, rationally select and determine the scientific evaluation method. Each of the aforementioned five different types of evaluation methods has its own advantages and disadvantages, and when evaluating, one should take aim at the specific situation to select the appropriate evaluation method. Amongst them, the evaluations of the multi-attribute utility analysis method, the fuzzy synthetic analysis method, and the grey correlation evaluation method have more precision but there are more restrictions of conditions and difficulties in specific implementation. The computer simulation method is the most commonly applied joint campaign IO effectiveness evaluation, it is a more scientific and objective method but building of models is difficult. The live-force exercise and training evaluation method is the most objective and most real method for conducting evaluations of joint campaign IO effectiveness, but it is most costly and its implementation more difficult. Consequently, when determining the effectiveness evaluation method, one should combine a variety of methods and not rely on one method; this ensures for scientific and rational organization and implementation of joint campaign IO effectiveness evaluation and ultimately being able to achieve evaluation results that draws on strong points and offsets the weak points.
[End of page 337]

II. Organizing and implementing evaluations…338

After determining the joint campaign IO effectiveness evaluation method, one should, in accordance with evaluation principles and basic steps, scientifically organize and implement. Below we use the computer simulation method as an example to conduct a study on organizing and implementing the joint campaign IO effectiveness evaluation. Utilizing the computer simulation method to conduct an evaluation of joint campaign IO effectiveness includes the four links of determining the personnel and equipment participating in the evaluation; formulating the joint campaign IO scenarios {*xiangding*}, building joint campaign IO models and conducting simulation evaluations.

(1) Determining personnel and equipment participating in evaluations

The personnel composition of computer simulation of joint campaign IO effectiveness evaluations basically should include: management personnel, players – the opposing sides, scientific research personnel, supplemental personnel[20]. Management personnel includes directing {*daoyan*}, judging {*caipan*} and controlling {*kongzhi*} personnel, the director is the leader for the entirety of management work. The role of management personnel is like that the directors and referees of sports competitions. Those being trained are divided into blue force personnel and red force personnel. The scientific workers in the computer simulation process involved in research and analytical work are the core of the computer simulation work. Before simulation starts, one should collect data in accordance with the goals and requirements of joint campaign IO simulations, conduct simulation model designs, provide the designed simulation models to the computer and network environments, and conduct software system design, launches, and setup and testing of a given computer and network environment. Supplemental personnel need to be familiar with using maps, military logistic services and computers, and they must also possess administrative office skills to help complete any joint campaign IO computer simulation work.

On the basis of specific situations of joint campaign IO effectiveness evaluation computer simulations, equipment participating in setup and testing normally include: large screen displays, computer local area network, **[end of page 338]** various computer workstations and microcomputer equipment, keyboards, digitizers (used to input and orient map information), and content such as graphical input and output devices as well as IO weapons and equipment, etc.

(2) Formulating joint campaign IO scenarios

Through the joint campaign IO scenario, one can describe the complex operational environment, the operational course, command and control as well as some detailed problems such as military strengths and logistic support that can be committed, initial combat level {*chushi zhandou shuiping*}, and battlefield postures such as time sequence of local momentum development, and one can illustrate the operational tasks and objectives. In formulating the joint campaign IO scenarios, one should pay attention to the following points: first, give prominence to the description of the constituting essential factors of joint campaign IO effectiveness evaluation; second, give prominence to the description of the joint campaign IO posture and battlefield information environment; third, stay as close as possible to live combat.

---

[20] Xu Xuewen {徐学文} and Wang Shouyun {王寿云}: *Modern Operational Simulations*, Science Press, 2001, p. 28

(3) Building joint campaign IO models

Building joint campaign IO models is a critical link in evaluating joint campaign IO effectiveness, and it is the core for establishing the application rules-regulations of each information, information system and IO weapon and equipment. For joint campaign IO, one normally should build the operational environment model, command and control process model, electronic warfare model, network warfare model, and psychological warfare model.

1. Operational environment model

The joint campaign IO environment affects the bringing into play of joint campaign IO effectiveness, and there are many factors involved in building a joint campaign IO environment model: first is terrain quantification model {*dixing lianghua moxing*}. Terrain status {*dixing zhuangkuang*} is an important factor for bringing into play joint campaign information systems and information weapon tactical and technical characteristics, so the precision level of terrain quantification directly affects the results of joint campaign IO effectiveness evaluations. When analyzing terrain factors, one must first determine the battlefield campaign or tactical operations area {*difu*}, and based on the characteristics of joint campaign IO, one can divide the terrain into summary description areas/zones {*gailue miaoshu quyu*} and detailed description areas/zones {*xiangxi miaoshu quyu*}. Second is the fortification works and obstacle model. **[End of page 339]** Both sides in joint campaign operations need fortification works and obstacles to protect their joint campaign information systems and weapon platforms, and constructing models of fortification works and obstacles are also extremely important, so one can conduct a differentiation of fortification work levels and natural obstacle and man-made obstacle levels. Third is the weather conditions model. The weather condition under joint campaign IO conditions is very important. Evaluating joint campaign IO effectiveness must fully consider weather conditions. Fourth is the electromagnetic environment model. When describing the electromagnetic environment, one mainly considers: the density of electromagnetic wave signals within a unit of time and unit of space; a signal based on the distribution status of frequency, power and signal form; a signal's attributes for both sides [enemy and us]. Fifth is a computer network environment model. One mainly considers a network's topology [structure] {*wangluo tuopu jiegou*}; topology [structure] nodes and exchange mode *tixi* system structure and protocols; circuit transmission capacity; and network security *tixi* system structure.

2. Command and control process model

The command and control process is the general designation for the activity conducted by a commander for assessing the situations, setting the resolution, formulating the plan and issuing orders, and it is a critical link for bringing joint campaign IO effectiveness into play. During operations simulation models, building a command and control model mainly includes: command and control order, battlefield posture and intelligence processing models. First is the command and control order

model. This mainly includes the various categories, contents and forms {*geshi*} in the organizing phase and implementation phase of joint campaign IO. During its design, one ordinarily puts together the command documents {指挥文书集 *zhihui wenshu ji*}, including the textual forms for the various documents that would be used in operations; then put together the command orders {指挥命令集 *zhihui mingling ji*}, conduct a break down {*fenjie*} of the various command orders, create a series of concise sub-orders {*zi mingling*} that contain independent activities, and thus form the orders {*mingling ji*}; and finally put together the database structure of command orders, list the entire parameters and data categories of each command order and form the data structure of command orders. Second is the battlefield posture model {*zhanchang taishi moxing*}. This includes the various situations or postures that may occur prior to combat and during combat in joint campaign IO and the composition essential factors and essential factor values of these postures. During model-building and design, one normally expresses this with the form of the battlefield report {*zhanchang baogao*}, similar with the design of the command order[s], **[end of page 340]** but one does not break down {*fenjie*} the report document. The battlefield posture must have a specific logical relationship with the command order, whereby one must design a host of corresponding reports and orders for a given type of posture. Third is the intelligence processing model {q*ingbao chuli moxing*}. Intelligence processing model-building is very complex and one can use the intelligence processing expert system method {*qingbao chuli zhuanjia xitong de fangfa*}; this is where one takes the information and battlefield posture acquired in reconnaissance of the joint campaign and uses it as the evaluation conditions, and undergoing the assessment of an expert system, one outputs an assessment conclusion of battlefield posture. The crux of intelligence processing model-building {*goumo*} is to construct {*goujian*} the rules database {*guize ku*} in the expert system.

3. Electronic warfare model

The electronic warfare model mainly includes: first is the electronic confrontation reconnaissance model {*dianzi duikang zhencha moxing*}. This mainly is to calculate the probability of gathering enemy intelligence such as their electronic equipment's tactical, technical characteristic parameters and location data. In specific terms, with the foundation of electronic confrontation reconnaissance equipment's indices such as reconnaissance distances {*zhencha juli*}, reconnaissance early warning times, reconnaissance response times, reconnaissance ranges {*zhencha fanwei*} and based on the associated order parameters and battlefield associated postures during the course of command and control, one seeks to gather the associated intelligence probabilities. Second is the electronic attack model. This mainly is calculating the size of the shape of jamming suppression area {*ganrao yazhi qu*} during electronic jamming. The foundation of the model is the indices such as frequency bands, ranges and jamming power of electronic jamming. Third is the electronic defense model. This model is achieved through the modeling of the aforementioned two areas, namely after using electronic defense measures, this is the enemy's decreased level of electronic reconnaissance and electronic jamming effectiveness against us. During model-building, this is mainly based

on the electronic equipment *tizhi* system's time selection quality, space selection quality, power selection quality and frequency selection quality.

4. Computer network warfare model

The computer network warfare model mainly includes the two aspects of network attack and network defense. The first is the network attack model. This is mainly conducting an analysis of computer attack weapon tactical and technical characteristics with the indices of penetrating and disrupting the opponent's network probability and disruption level. During model-building, one should separate the different encryption level networks for study. Second is **[end of page 341]** the network defense model. This mainly is to analyze the network's security, and this mainly includes content in several aspects such as the network's physical parts, software, data and security management, etc.

5. Psychological warfare model

The psychological warfare model mainly includes the two aspects of psychological attack and psychological defense. The first is the psychological attack model. This mainly is to conduct an analysis of various psychological warfare means adopted when attacking the enemy's psychology, such as utilizing television, broadcasts, leaflets and electronic mail, as well as information beneficial to oneself that can be distributed in large volumes with indices such as to cause the enemy commander difficulty to correctly make decisions, to bring down morale, create nervousness, worry, fear, weariness, and other unsatisfactory of war-weariness levels. Second is the psychological defense model. This mainly is to conduct an analysis of various psychological warfare means adopted to preserve one's own force's psychology and morale, and the indices are the levels of raising and protecting one's own commanders' and soldiers' morale.

(4) Conducting simulation evaluations for operational effectiveness

The final link of the joint campaign IO effectiveness evaluation is to conduct simulation evaluations, and this is mainly in three phases: the preparations phase, simulation phase and analysis phase.[21] The main work of the preparations phase are in aspects such as determining objectives, clarifying forms, general design, conducting data inputs, preparing equipment, modeling and software, organizing of personnel, logistic support, preparations of associated specialized data-materials such as scenarios, etc.,

[21] Xu Xuewen {徐学文} and Wang Shouyun {王寿云}: *Modern Operational Simulations*, Science Press, 2001, p. 31.

monitoring characteristics {*jiance xingneng*}, and completing set-up and tests {*tiaoshi*}. The Guidance and Regulating Office {导调室 *daotiaoshi*} is responsible for regulating-controlling {*tiaokong*} the simulation phase, and the red and blue sides conduct a series of rounds-type simulation. The analysis phase is mainly an analysis of the IO simulation data. The form for the results of the analysis phase is normally a report.

III. Utilizing the evaluation conclusion…342

The goal of the joint campaign IO effectiveness evaluation is to conduct **[end of page 342]** a thorough summary analysis of the evaluation conclusion so as to, in the end, effectively utilize it. The utilization of the joint campaign IO effectiveness evaluation conclusion is to undergo a summary analysis of the evaluation conclusion and improve the accuracy of the evaluation.

(1) Revision model

When conducting analysis of the effectiveness evaluation conclusion, one frequently discovers inconsistencies between the evaluation results and human predicted results. Through analysis of the evaluation conclusion, one can find the specific reasons for triggering model and parameter setup inaccuracies, improve the bonding degree of the model and actual battlefield, make adjustments in the model and re-set up the model parameters.

(2) Improve command and control capability

Through the operational effectiveness evaluation conclusion, one can analyze the problems appearing during the course of decision-making, planning and controlling by the joint campaign IO commander and his command organ, as well as expose insufficient shortcomings, objectively summarize lessons, so as to allow their acknowledgements to be elevated and improve command and control capabilities of commanders and their command organs.

(3) Improve unit integrated-whole operational capability

Through the evaluation of joint campaign IO effectiveness, one can discover the critical links and each factor affecting one's joint campaign IO capability, find the strong points and weak points, and further improve a unit's integrated-whole operational capability. **[End of page 343]**

This page intentionally left blank.

Chapter 21
Joint Campaign Information Operations Training…344

The information operations training is the live exercises and activities for the training of the information operations understanding, skills, and capabilities, that are implemented in a planned, organized, and targeted fashion, for each level of commander of the joint campaign, and each level of the corresponding military (branch) command agency. Its objective is to increase the joint campaign information operations capabilities. With regard to enhancing the information operations training, it is a major component of the joint campaign training, under information technology conditions, and it is also a major measure for increasing the joint campaign combat capabilities.

Section 1: Characteristics of Joint Campaign Information Operations Training…344

The information operations training serves as an important component of the joint campaign training, but it is different than the military training under normal conditions, because it has different characteristics and requirements. They are mainly displayed in the following several aspects.

I. The blended quality of the training topics…344

With regard to the combat under information technology conditions, the distinction between the information and weapons, and the control systems and the casualty style weapons can be combined into one entity, the information combat operations and the other combat measures can naturally be combined, and therefore, this causes the information operations to be carried out in the entire process of the combat. The combat operations cannot be separated from the support of the information operations, and this determines that the information operations training is not just **[end of page 344]** an aggressive, isolated, and specialized training topic, but it must also be implemented in the whole process of the joint training. Within the blending of the training on the other topics, this can then fully be implemented through the entire training of the information operations training.

II. The open quality of the forces participating in the training…345

Between the complex spaces of the wide electromagnetic spaces, computer network spaces, and psychological spaces, the information combat operations cover all of the battlefields in the land, sea, air, and space dimensions, which causes the forces that are participating in the information operations to not only receive the various restrictions of the other combat operations but it also forces the military troops and locals to also participate. On another hand, with regard to each of the information combat operations, why should they fear the minute operations, which could be dragged into each of the forces of the information operations? In addition to the current situation, they also have

depth, and in addition to their own specialty, they also have the other specialties, and they do not have the division of the front and rear lines. Therefore, the characteristics of this type of wide area force participating in the information operations causes the information operations training to also have a very strong open quality, and if the forces participate in the information operations, then they must participate in the information operations training.

III. The synthesized quality of the training content…345

Although we are currently facing a transition period of shifting from mechanized war to information technology war, there are differences in the period of use of the focal points and the degree of integration for the information operations soft kill and hard destruction, but the implementation of the measures of information operations is fundamentally determined. For example, the information attack operations jointly use the electronic interference, military deception, network attacks, entity destruction, psychological warfare, and other various types of measures to reduce and destroy the effective use of the enemy information systems, and furthermore, each of the measures used in the information operations also includes various types of combat operations. The multitude of information operations measures creates the content of the information operations training, and it also is correspondingly complex. Therefore, during the arrangement of the information operations training content, they must train on each of the types of combat measures and operations, and they cannot just simply add to the several current types of combat measures. Moreover, based on the unified combat objectives, they must be jointly coordinated and they must be coordinated identically in order to implement the synthesized quality of the training. **[end of page 345]**

IV. The flexibility of the training methods…346

The digital troops and the information network battlefields are in agreement with one another, and through the wireless communications, optical fiber communications, satellite communications, and other transmission measures, they put the battlefield command agencies, combat troops, logistics support troops, single weaponry, and single troops into a crisscrossed information network space. Through the collection, submission, and processing of the battlefield information, it can describe a commonly used battlefield situation that corresponds to the battlefield, which allows each level of commander and staff officer personnel to achieve the requirements for a clear, accurate, and appropriate battlefield situation diagram, from the shared databases, and this puts forth decisions and the command troop operations. This significantly reduces the cycle of the distance between the commander decision-makers and the combat troops, as well as the adoption of the operations, so they are capable of implementing effective information combat commands. This characteristic of the digital troops allows the information operations training to achieve the close reciprocal relationship between the troops that rely upon digital [information] and the command agencies, which uses simulations, and lifelike actual technology that is even more flexible, as well as other types of organized training, and it also can guarantee the results and effectiveness of the training.

V. The precision quality of the training assessments…346

The information technology of the weaponry is the physical foundation of the information operations. The combination of the information technology and the weaponry forms an information technology weapons system, it includes each of the combat platforms and guided missile systems, etc. and with the command information systems, it forms the main methods for the information operations. The information technology weaponry allows the information flow of the information operations to objectively, accurately, and rapidly lead to the collection, transmission, and processing of the information in the information networks, and this characteristic allows the assessment of the information operations training to reach even greater heights. The proportion of the quantitative assessment will significantly increase and the precision of the training assessments will greatly increase.

VI. The complexity of the training environment set-up…346

The emergence of information operations was the broad use of a series of highly technological results in the military realm, which regarded information technology as the core and it was a combat style that contained a large amount of advanced science and technology. With regard to the comparison with the traditional mobilization combat and firepower combat operations, most of the information combat operations **[end of page 346]** are developed within the intangible electromagnetic spaces, computer network spaces, and the space of man's knowledge. This puts forth even higher requirements on the training environment, and furthermore, it also requires them to gain the support of the technology and monetary resources. They should also be aware that the multi-dimensionality of the information operations spaces, the variety of the forces participating in the combat, the diversity in the combat styles, and the combat of the combat operations sets up an even greater degree of difficulty for the environments of the information operations training.

Section 2: The Content of the Joint Campaign Information Operations Training…347

The content of the information operations training refers to the integration of each type of knowledge and capability that the trainees should study and master during the process of the information operations training. The content of the information operations training should be determined based on the joint campaign information operations tasks, the systems and organizations of the troops, as well as the possible development of the weaponry. The scientific set up of the information operations training content is a guarantee for the training of qualified information operations commanders, as well as their corresponding command agency personnel. The content of the information operations training is reflected through the information operations training plans, the training outlines, the teaching materials, the scenarios, and other forms. The content of the information operations training is not unalterable, but it continuously develops following the changes in the joint campaign styles, the development of the weaponry, and

the newer modern eras. The content of the joint campaign information operations training can normally be divided into the information operations training of the joint campaign commanders and their command organizations, the training of the information operations specialized troops (elements), as well as the information operations training of the joint campaign military groups and the other troops, and other aspects.

I. The content of the commander and command organization information operations training…347

The joint campaign commanders and command organizations are the organizers and commanders of the information operations and the quality is the determining factor that restricts the success or failure of the information operations. Because of this, during the organization of the information operations training, they must focus on making great efforts in the training of the joint campaign commanders and the **[end of page 347]** staff officer personnel from the information operations command agencies. They should focus on studying and mastering the following content.

(1) The fundamental theories of the information operations

Most importantly, they should understand and grasp the concept of the information operations, the principles and characteristics, the information operations types and styles, the information operations guiding ideologies and fundamental principles, the information operations forces structure, the information operations fighting methods, the organization and planning of the information operations, the command and control of the information operations, the information operations support, as well as the information operations construction and development, and other theoretical issues. They must also understand and research the foreign military information operations theoretical research situations, and they must become familiar with the forward position theoretical issues of the foreign military information operations.

(2) The technology theories of the information operations

First of all, they should understand the microelectronic technology, photoelectricity technology, superconduction electronic technology, sub electronic technology, energy technology, and other foundational technology, of the information operations. Second of all, they should master the information collection technology, information transmission technology, information processing and regeneration technology, control technology, information attack technology, information defense technology, and other major information operations technology. Third, they should understand the system structure technology, the connection and linking technology, the system integration technology, the simulation and evaluation technology, the integrated application technology, and other general information operations technology. In addition, they must also understand the status and developmental trends, etc. of the information operations technology equipment of the combat opponents or of the potential opponents.

(3) The application theories of the information operations

First of all, they must understand the fundamental viewpoints of the military information operations, the situation of the fundamental structure of the information systems, the organizational equipment and information operations capabilities of the information operations forces, and the operations and methods of the information operations. Second of all, they must become familiar with the organization equipment, combat capabilities, and the possible tasks and application methods of the information operations. Third, they must master the methods of the information operations organization and the implementation of each of the combat types in the joint campaign.

With regard to the information operations commanders and their command agencies, and with regard to the foundation of the above-mentioned training content, **[end of page 348]** they must also focus on implementing the organized command training of the information operations. Its content mainly includes: the first is understanding the intentions of the leadership of the upper level authorities and the tasks that the authorities at the same level are responsible for. The second is the capability of analyzing the battlefield information environments and assessing the information operations of the Chinese and the enemy. This includes the analysis of the structural situations of the information systems of the enemy and of the Chinese, the information defense capabilities, and the strong and weak points; the analysis of the quantity and quality of the information attack weaponry of both the enemy and the Chinese, as well as the information attack capabilities; the enemy information attack plots; the primary direction, primary methods, and primary measures; the analysis of the structure of the infrastructure of the both the enemy and the Chinese, as well as the influence of the support information operations strengths of the people, etc. The third is the information combat and command policies. This mainly includes the issues that the policy makers must focus on. The fourth is the formulation of the information operations plans. This is mainly the mastery of the methods based on the decisions of the upper level commanders, the tasks of the information operations at the same level, the information operations decisions, and the formulation of the information operations plans. The fifth is the training of the formulation of the joint plans of the information operations. This is mainly the mastery and formulation of the coordinated planning of each period of tasks and operational methods of the information operations on each of the combat forces, between the information defense and information attacks, between each of the groups of the information combat operations, as well as between the information combat operations and the other combat operations.

II. The training of the information operations specialized units (elements)…359

The information operations specialized units (elements) are a main force in the implementation of the information operations, and therefore, they are also a focal point for the information operations training. The specialized structure of the information operations specialized units (elements) is complex, it includes the reconnaissance intelligence troops (elements) that are responsible for the collection of information, but it

also includes the electronic warfare, network warfare, and psychological warfare troops (elements) that are responsible for the information attacks. Based on the different types of specialties, the implementation of the content of the training and the methods for each are different.

(1) The specialized training for the information operations specialized troops (elements)

1. The specialized training of the electronic warfare troops (elements)

The electronic warfare troops (elements) that are subordinate to the joint campaign military groups are the main force for implementing the information operations, and they mainly implement the foundational knowledge and studies of the electronic warfare and the technology and the war tactics training **[end of page 349]**. The content mainly includes: the structure, functions, work principles, and work methods of the electronic equipment of the Chinese military; the characteristics, tasks, guiding ideology, and fundamental principles of the electronic warfare of the Chinese military; the fundamental military tactics and the specific measures and methods of each type of situation of the Chinese military electronic warfare; the command and coordination of the Chinese military electronic combat; and the organization and implementation of the electronic warfare of the Chinese military under each type of operations style. Another focal point is the electronic interference training. The objective of the electronic interference training is to master the use of each type of electronic interference war tactic. It can mainly be divided into the suppression electronic interference training and the deception electronic interference training. The objective of the suppression electronic interference training is to increase the capabilities for information collection, information transmission, and information processing that can weaken and cripple the information systems and information weapons of the enemy; this mainly includes the communications interference training, the radar interference training, the photoelectricity interference training, the control and guided interference training, the navigation interference training, the detonator interference training, the identification of friend or foe interference training, etc. The specific content of the communications interference training includes: the first is the applied training on the width of the jammer spectrum; the second is the training on the jamming signal adjustment methods and styles; the third is the applied training on the function intensity; the fourth is the designation training on the radiation direction; the fifth is the elective training on the frequency or wave band. The main content of the radar interference training includes: training on the chaff dispersing (interference wire / band), training on the placement of the reflector, the training on absorbing the layer coating, the training for setting up the decoys and radar bait, and the electronic function training for changing the mediums in the local air space. The main content of the photoelectricity interference training is the training on the laser interference, which is the use of an extremely bright laser for interference, the photoelectricity apparatus used to destroy the enemy, or to interfere with or damage the eyes of the enemy personnel, which is a method that blinds the enemy personnel and instruments so they are blind. It can be

divided into the direct interference training, the training to mislead the interference, the scattered interference training, the passive interference training, etc.

With regard to the deception type electronic interference training, it is the training that uses their own electronic equipment or camouflaged equipment to put out false information, or it passes off as the enemy reports and intelligence that are broadcast, or the implementation of false communications, the set up of false electronic targets, etc., or the use of electronic equipment and electronic technology measures, to deceive or mislead the enemy personnel in the realm of electronics; the content of the training for the deception style radar interference mainly includes: **[end of page 350]** the training on remote deception interference, the training on angular deception interference, the training on speed deception training, etc.

2. The training of the network warfare units (elements)

The network warfare units (elements) are a major force in the implementation of the battlefield network attacks. The network warfare units (elements) should mainly implement the network reconnaissance and network attack training, based on understanding and mastering the structure, equipment models, equipment function standards, network protocols, network operations systems, and network management of the enemy military computer information networks, as well as the combination of the military networks and civilian networks.

The content of the network reconnaissance training mainly includes: network eavesdropping, command decoding, registering the computer networks, information flow analysis, target system security scanning, the collection and analysis of the leak of electromagnetic information, etc.

The content of the network attack training is mainly the training on the computer virus attacks and the training on the computer network invasions. The training on the computer virus attacks is mainly the study and compilation of each type of different characteristics of the virus destruction procedures, on the foundation of mastering the virus destruction mechanisms, characteristics, as well as the symptoms, studying how the virus or invasion will be implemented, how the control of the virus will break out, as well as the use of the mastery of the attack opportunities and the attack methods. The computer network invasion training is mainly the training for how to invade the enemy computer networks, how to decipher data, how to implement attacks against networks, etc. The main content includes: 1) Suspension training. The training that implements destruction on the computer network system nodes and the training that suspends the information transmission circuits. 2) Distortion training. This is mainly the training on changing the data value of certain data and documents, or improving certain procedures, or fixing the content of some of the information. 3) Posing training. This is mainly the method of training for posing as the enemy upper level authority or the subordinates, in order to enter into the enemy information systems and to master and create the skills of confusion **[end of page 351]**.

(2) The joint training of the information operations specialized units (elements)

The information operations joint training is the training that increases the joint campaign information operations capabilities, integrates the scattered information operations forces and the corresponding elements, and focuses on striving for and maintaining the battlefield information dominance, and implements a high degree of integration.

1. Common fundamental training

The main content includes: the foundational knowledge, theories, and skills of the joint campaign information operations, the awareness training of the joint campaign information operations, the formation of appropriate joint campaign fighting ideological and operational functions.

2. Mobilization training

This mainly refers to the training of the information operations troops, based on the joint operations command orders, and the other military services, which commonly implement the mobilization from the realm of waiting for an opportunity to the realm of predetermined operations. The specific training content includes: march organizations, motorized mobilization, railway (airborne) transport, air defense and anti-nuclear and biological attacks, troops quickly occupying the battlefield and organizing the development, electronic camouflage and battlefield protection, etc.

3. Information reconnaissance training

This mainly refers to the training of the information reconnaissance, transmission, integration, distribution, and use for the information operations troops and the other troops. The main content includes: implementing training on the information collection, transmission, identification and blended skills for each of the reconnaissance troops of the communications combat swarms; the training implemented on blending the skills of the intelligence collection, transmission, and identification for each reconnaissance troop of the radar combat swarm; the training implemented on integrating the handling of the intelligence exchange and the contrasting verification for the communications combat swarm and the radar combat swarm; the training that integrates the handling of the intelligence exchange and the contrasting verification between the electronic combat swarms, and the other forces and the technology reconnaissance forces.

4. Combat and command training

This mainly refers to the combat and command training of the information operations groups (swarms), under the unified command of the joint commands **[end of page 352]**. The main content includes: the training of the command post (system) development and connection; the training of the communications combat swarms and the

connection, communications, and operations with the radar combat swarms; the training of the electronics combat group (systems) command flow and the coordinated command training, etc.

5. The integrated information operations training

This mainly refers to the entire training implemented between the command information networks and the support troops, and on the information operations troops professional departments and their use. The main content includes: the internal coordinated training of the information operations integrated support systems and the information sharing and joint support training between the information operations integrated support systems, the higher level authority support systems, and the other support systems, etc.

6. The joint information operations training

This mainly refers to the reconnaissance and interference training implemented on each type of enemy information systems, based on the different procedures of the joint campaign, and the integrated use of each of the information operations forces. The main content includes: the coordinated reconnaissance interference training of each of the groups, the interference training under the intelligence support of each group, and the joint attack and joint defense training, etc. for the electronics combat groups and the other military services, under the joint campaign background.

7. The joint information operations live troop exercises

This is mainly the overall training that revolves around the offense and defense of the battlefield control for dominance and development. It fundamental content includes: the first is the training that focuses on achieving the connection, communications, and mutual operations of the information resource sharing, the characteristics of command integration, the focus on the intelligence and information systems, the intelligence operations command and control systems, the firepower attack systems, and the integrated support systems within the joint information operations system; the second is the training that focuses on the characteristics of effective, real time command and coordination in the joint information operations systems, and focusing on each of the command structures and the command personnel's use of command networks and command automated systems, in order to implement active policy making, quick coordination, joint commands, and real time control; the third is focusing on regarding the inspection of the information flow and the mixture of the process of each of the information combat modules and information combat elements as the objective, **[end of page 353]** as well as implementing the integrated exercises, campaign, and military tactics exercises in subscales, subtopics, subphases, and sublevels.

III. The information operations training of the other units of the joint campaign…354

The main task of the other military units of the joint campaign within the information operations is to implement information defense. Therefore, the focus of the information operations training is to increase the "training on the five defenses."

(1) The anti-information reconnaissance training

This mainly includes the anti-information reconnaissance training of the combat deployments and operations, and the anti-reconnaissance monitoring training of the combat information. The anti-monitoring training of the combat deployments and operations is mainly the training of the troops that implements camouflage and early warning defenses, and it prevents the enemy personnel from acquiring the intelligence and information from the Chinese military combat deployments operations. The camouflage training includes: using the topography and the poor climate to disguise; constructing fortifications in order to implement the camouflage; making reasonable deployments, scattering the deployments, and spreading out the operations; using smoke screens, camouflage, the concealment of the manpower, using vegetation to conceal the manpower, and changing the external form of the objectives and the electromagnetic radiation characteristics, as well as other methods in order to camouflage; setting up decoys, creating false operations to deceive the enemy personnel, etc. The early warning defense training includes: the methods for organizing defenses against airborne investigation and reporting networks and ground early warning.

The anti-reconnaissance monitoring training of the information operations is mainly the confidentiality training of the communications signals. The content includes: (1) Information encryption training, which is the information camouflage training that implements the alterations of the information, from being obvious to secretive. (2) The information differentiation training, which is the training that is implemented to verify the legality and effectiveness of the system or network information exchanges, and the accuracy of the information being exchanged. This includes three types of training, which are the differentiation of documents and reports, the differentiation of the identities, and the digital signatures. The training on the differentiation of documents and reports, first of all, is the differentiation of the content of the documents and reports, which implements training on the agreed upon encryption; second of all, it is the differentiation of the original source of the documents and reports (outgoing messages), which implements training on the agreed upon data encryption ciphers and implements training on the agreed upon transmission of the documents and reports; thirdly, it is the differentiation of the time of the documents and reports, which implements training on the transmission time procedures of the documents and reports. The training on the identification differentiation includes the differentiation and the verification training. The differentiation is mainly the training on the confirmation methods on the person entering the system and the verification primary training is the method for implementing differentiation on the true or false identities entering the system **[end of page 354]**. With

regard to the identification differentiation methods: the first is the differentiation of the commands, the second is the differentiation of the magnetic card, and the third is the differentiation of the biological characteristics, such as confirming the differentiation of the identities through the verification of people's fingerprints, retinas, speech, or handwriting, and other physical characteristics. (3) The information control training, which is the training for implementing control on the user's application of the information systems or the information system resources. It mainly includes two types, the browsing control training and the command control training. The browsing control training is the training that implements limits on the browsing operations, as well as mastering the implementation of the limits of the browsing operations of the authorized user entering the computer network systems; the command control training is the differentiation training implemented on the established commands and the transmissions. (4) The information blocking training. This is the training that restricts the transmission of information. They must be adept at limiting the transmission of the information within the regions and time frames, in order to reduce the scope of the scatter, within the communications systems. For example, it is implemented on the wireless communications, the control and implementation of silence, etc., on the communications power. (5) The training of the information camouflage. The training uses strategic measures to create false information, and it is adept at creating each type of false information on the communications systems, in order to camouflage their own true operations, and this is mainly the training that opens up the communications systems of the false information or creates changes in the information. For example, it is implemented in the wireless communications, which is the training that implements sudden fluctuations on the information from certain directions. The information simulation training is mainly the training that implements the mutual exchange of accurate and false information in the communications systems. (6) The training on information obstruction. This is the transmission of large amounts of false information and useless information on the information communications. (7) The training on multi-channel transmission. This is the training method used to provide multiple transmission channels (information channels or circuits) for the same information. For example, on the wireless communications, the organized training implemented on the area communications networks, the concealed networks, the complex networks, the backup networks, the logistics networks, and the on-duty networks.

(2) The training on the anti-electronic attacks

The joint campaign military troops use large amounts of wireless broadcasting stations, radars, and other electronic information equipment, and it is a major objective of electronic attacks from the enemy. Therefore, the anti-electronic attack training is the major content of this training. Apart from implementing the anti-electronic attack technology training on the personnel that will be operating and using the electronic information equipment, **[end of page 355]** they should focus on organizing the anti-electronic attack technology training well. This includes the wireless communications anti-interference, radar anti-interference, and anti-photoelectricity interference training.

The wireless communications anti-interference training. This is mainly the training that flexibly uses the anti-electronic interference on the communications equipment, such as changing the work frequencies and increasing the radiation signal strength; establishing the concealment of the wireless communications networks (outgoing) and using the anti-interference specialized connection documents; establishing logistics wireless communications networks (outgoing) or complex wireless communications; training on the suppression or destruction interference source methods, etc.

The radar anti-interference training. This is mainly the training on the reasonable deployment of the radar network anti-electronic interference; the training reasonably deploys the different frequency bands and the different radar systems and organizes them into radar networks; the training uses multiple types of reconnaissance equipment and sensors; the training combines the methods of the operating technology of the anti-interference, the anti-interference by changing the frequency, the anti-interference by changing the work systems, the users concealing the work strength, the use of the blind angle of the interference beams to implement probing, and other methods, during the implementation of anti-interference on the anti-interference circuits and devices being used.

The training of the anti-interference on the photoelectricity equipment. This mainly includes the training that reasonably deploys photoelectricity equipment and materials, and conceals the use of the photoelectricity equipment and materials, etc.

(3) The training on the anti-network attacks

1. The training on the anti-computer virus violations

The most important software and hardware entities on the networks are the servers and work stations. Because of this, the key to the anti-computer virus violations training is to conduct training on the anti-virus procedures of the work stations and servers. The work station anti-virus infection training is mainly the training on the software virus monitoring and removal; and the use of installing anti-virus chips, etc. on the computer virus cards and network interfaces. The server anti-virus training is mainly the training on the use of the possible anti-virus [software] that can be loaded onto the modules. **[end of page 356]**

2. The training on the anti-computer network infiltrations

The main point of the anti-computer network infiltration training is the defense against illegal invasions. The main training is the use of the network anti-firewall technology. In addition, they also must train on how to avoid electronic interference, and implement electronic screens and prevent the unintentional leak of electromagnetic signals, as well as training on how to implement encryption on the systems and data, and

other measures, in order to guarantee the overall reliability of the operational security and data of the systems.

(4) The training of the anti-psychological attacks

With regard to the training of the psychological defenses, the fundamental objectives are to increase the psychological skills of the trainees, to guarantee the normal activities under combat conditions, and to bring out each type of combat capabilities of the trainees, to the maximum degree possible. Based on the actual situation of the Chinese military, the content of the psychological defense training is mainly implemented in the following training, on the foundation that they understand the equipment and technology of the foreign military psychological warfare, the combat technology functions, and the combat application methods:

1. Battlefield simulation trainings

With regard to the battlefield situations that are set up in an objective and focused manner, they simulate the live battlefield environments and situations, which allows the trainees to experience a certain degree of the psychological stimulation of the combat elements, thereby increasing their psychological activity levels, and enhancing their psychological adaptations, responsibilities, and self-control capabilities.

(i) Battlefield scene simulations

The possible sounds, lights, smoke, electronics, and other results that can occur on the simulated battlefield pretty accurately play up the battlefield atmosphere, which stimulates the feelings of the sights, sounds, and smells of the trainees, which allows the trainees to have an actual battlefield situation that they are facing, and they can gradually adapt to these battlefield situations, thereby reducing the psychological weight that it can bring.

(ii) Battlefield psychological simulations

The set up of the complex and ever-changing enemy situations increases the degree of danger of the combat circumstances, and with regard to the set up of the dangerous obstacles, it increases the capabilities for psychologically adapting to each type of interference elements, and trains the trainees in complex and **[end of page 357]** dangerous situations.

(iii) Strong battlefield stimulation simulations

For example, if we let the trainees enter into a secure fortification that has a secure protective layer, then they can carry out an artillery cover attack, and experience the tense feelings and terror of the artillery raids. They must arrange the training under

dangerous conditions, such as the training that exists in the field, night time training, organized troops participating in rescues, implementing each type of critical and emergency tasks, etc.

2. The training that exists in the field

Throwing the trainees into dense forests, isolated islands, deserts, the Gobi desert, and other extremely harsh environments, allows the trainees to experience the positive influence of the harsh natural conditions; throwing the trainees into environments of live exercises allows the trainees to personally feel the threat of death; putting the trainees into isolated and helpless environments, with limited food and water, allows the trainees to experience the trials of life and death and to temper themselves to strengthen their willpower and enhance their stamina. When the situations allow, they can also arrange and organize the trainee implementation of parachute, diving in shallow seas, cave exploration, rowing a dugout canoe, climbing scaling ladders, and other training.

3. Self-adjustment training

With regard to leading the trainees, based on the training, the combat situations, as well as the characteristics of the changes in one's own psychological beliefs, they should adopt the measures of adjustment and control of their physiological beliefs, in a conscious and active way, in order to bring out and maintain psychological stability. For example, they can organize the trainees so that they consciously do a few psychologically relaxing activities, which will alleviate the degree of tension in their muscles, eliminate the tension or panic in their psychological feelings, and maintain their coordinated development of themselves. Within the gaps in the training and combat, they should appropriately do a few activities that relax their own muscles, such as push-ups, calisthenics, an appropriate amount of running and jumping, and other exercises that relax the muscles, in order to transform their tense psychological conditions. They can also implement trainings to desensitize their emotions and increase the psychological quality of the trainees. They can first allow the trainees to recall their experiences or all of the fearful situations that they have seen, in order to induce their production of tense feelings, and when these tense feelings reach a certain level, they can again lead them to recall these they can then think of the situations that are happy and relaxed which lead them to be happy, and thereby, vigorously use **[end of page 358]** these feelings to replace or extinguish the tense feelings.

(5) The anti-data destruction training

This mainly includes the reasonable and dispersed deployment of the electronic information equipment and materials, as well as the adoption of evasion activities, etc., in order to combat the data destruction methods that the enemy implements against the Chinese electromagnetic infrastructures and equipment.

Section 3: Joint Campaign Information Operations Training Methods…359

There are large differences that exist between each of the military services of the joint campaign information operations forces, between each of the specialties in the military services, and between each of the levels of the combat forces, in the organization and implementation of the information operations. This causes there to be differences between the information operations training and the other military training, in their degree of difficulty with the organization of the training. Therefore, the joint campaign information operations troops, with regard to the organization of their training, must combine the actual situations of their own units and the specialized areas that are subordinate to them, and they must combine each level of flexible and elective training organization methods in the training, in order to practically enhance the training effectiveness.

I. The collective deliberation style training…359

The collective deliberation style training refers to a type of method that organizes the information operations training through the assembly of the research, discussions, and other forms, and it is a format that focuses on implementing concentrated research and tackling the key problems in the areas of focus for the information operations exercises. The objective is to fully bring out the function of the wisdom of the group, and to work as a team to resolve the topics and points of difficulty. The first is that they must look for the main issues and difficulties in the information operations training. They must be involved in understanding and mastering the present conditions of the troop information operations training, they must genuinely analyze the key segments to restricting the information operations training of the troops, and they must establish objectives, content, methods, and steps of the deliberations, on this foundation. The second is that they must master the opportunities of the collective deliberations. The energy of the implications of the collective deliberations cadre backbone is quite large **[end of page 359]**, and it should not be organized often, but it should be implemented in key phases during the information operations phase training. This way, it will be convenient to go through the exercises promptly to discover and resolve the issues, and it is also convenient to promptly lead and deepen the next steps in the training. The third is that they must use the deliberation results to promptly guide the training exercises. They must promptly organize the implementation of the generalization scanning of the specialized people on the topics of the discussions. They must pull out the methods and measures for practical management and with the guided training exercises, and they must push the information operations training into deeper development.

II. The mutual help and mutual study mode training…360

The mutual help and mutual study mode training is the implementation of cyclical trainings to break through the restrictions of the current systems and specialties of the military services, to commonly use the information training resources, and to adopt the methods of going on visits to study and having guests come lecture. The first is that they

must development the mutual help and mutual study between the military areas. The military use information technology is developed on the foundation of the civilian use information technology, and the information technology is blend of military and civilian use. Therefore, the troops must actively put forth requirements with the local electronics, telecommunications, information engineering, and other institute (research institutes) systems, and based on the advanced technology superiority and rich resource forces, organize the studies and training. They must also provide exercise bases to the institutes and universities. The second is that they must develop the mutual help and mutual study between the specialties. The information operations trainings involve various types of military service specialties, and there is a high degree of scatter, especially in a few of the specialties of the smaller military services, and the training, organization, and support is difficult. Because of this, they can adopt measures that cross over the systems, are based on the specialties, and divide the regions, in order to organize each of the types of information operations specialized collective troops, in a more convenient way, in order to concentrate and organize the training, in order to mutually train on contract and in order to fully bring out the pros of each of the troops and to train the resources effectively. The third is that they must develop mutual help and mutual studies across the military services. Following the development of the Chinese military equipment technology, each type of new information operations equipment and materials has continuously been allocated to the troops. They must encourage breaking through the boundaries of the military services, expanding their development of the mutual help and mutual study between each of the military services and the military troops, they must organize the studies of new equipment and train on the opponents training and the corresponding coordination, and they must accomplish the common increase in the mutual training and benefits **[end of page 360]**.

III. The centralization of the base mode training…361

The centralization of the base mode training is a type of training method that uses the information operations training centers of the specialties, and rotates the training of each type of information operations personnel, in a planned fashion. This type of training center normally uses a complete set and a large scale of information operations training facilities and they can provide the information operations command personnel, specialized personnel, and information equipment operations within the applied training, with the implementation of theoretical research and discussions, on the information equipment operation functions and information combat, and technology functions. On one hand they must combine the actual situations of the training for all of the military information operations, and they must construct an information operations training center that has organized technology, war tactics training, and live troop exercise functions.

IV. The network system mode training…361

The network system mode training refers to the use of computer distribution network systems to implement information technology and tactical training. The general headquarters unified military training information networks and three networks, as well

as the local area networks that each of the troops and universities have established for the overall military, develop the integrated training of the information operations networks and create beneficial conditions. They must fully use the command automated established results that have already been established to significantly develop the networked training. On one hand they must develop the online exercises by mainly adopting the formats of single party technology work and the combat operations, based on the formulation and organization of single and multi stage online work, and they must temper and increase their leading cadre and organizational information operations capabilities; or they must implement multi military service, cross-system, and cross theater information operations specialized training or joint campaign topic exercises carried out by the general headquarters or the military region. On the other hand, they must develop the online schooling, which fully develops the use of each of the types of networks and databases of the Chinese military, sets up the networked universities, and organizes the online lectures, tutorials, studies, work, and other institute activities, in order to expand the aspects that receive study and to increase the network effectiveness **[end of page 361]**.

V. The live troop exercise mode training…362

The live troop exercises mode training is on-site live troop simulated operations exercises of the units (elements) of the upper levels that attend the training, under unified organization, that regard the joint operations as the background, and focus on the common training topics, in order to implement mutual hypotheses for the enemy conditions. The live troop mode training is the higher-level format of the information operations training, which is used in the overall training to increase the overall information operations capabilities of the troops. First of all, they must insist upon the principles of horizontal combinations and gradual combination. After the troops have accomplished the information operations fundamental task training tasks, each specialized troop can combine together. They must regard the elements as the units organizing their own level of military service specialized tactical and applied training, and they must organize from the single specialty to the multiple types of specialty layers, and from the single military services to the gradual integrated training of the various military services. This achieves the combination of the current technology measures and the tactical measures, in order to lay a foundation for the live troop joint exercises. Second of all, they must implement the objective and impartial result evaluations and rulings. Under the conditions of all of the services not unifying the information operations training evaluations standards, the result evaluations of the live troop joint formation exercises are a difficult point, so they must establish a scientific quantization evaluation standard, in order to strive for a transformation from the manmade evaluation and rulings to the computerized automated evaluations and rulings. The live troop joint exercises can adopt the integrated method of the manmade and computerized automated evaluations and rulings in order to implement tem, by using the objective and impartial evaluations and rulings.

Section 4: The Requirements of the Joint Campaign Information Operations Training…362

The joint campaign information operations training has highly scientific content, a vast scope of training involvement, high training environment set up requirements, highly difficult training result evaluations, and other characteristics. This puts forth even higher requirements for the information operations training. The requirements to make confirmations about and grasp the knowledge have an important significance to organizing the information operations training well. **[end of page 362]**

I. They must establish a scientific operating mechanism and strengthen the training supervision…363

First they must establish a unified and effective organized training structure. The organization, planning, coordination, and control of the information operations training are relatively complex systems. They should abide by the principles of "making the warfare and the training identical, and combining the wartime and peacetime." They should establish an information operations organized training structure and strive for making adaptions to the current command system. Normally the headquarters leadership takes the lead and the work training, intelligence, communications, information operations (electronic warfare), and the corresponding personnel from the artillery troop departments are the priority, they recruit the leadership from the other military services and departments to participate, and they guarantee the authoritativeness, comprehensiveness, and the coordination of the leadership structure. The second is that they must establish scientific regulations. Based on the requirements of the joint campaign for the information operations, and based on the training regulations, they must genuinely research the topics, content, division of order, quality standards, and reward and punishment measures, etc., in order to formulate the detailed principles to implement the training, and to standardize "who will do the training, how it will be trained, to what extent it will be studied," and other issues of the information operations training. They must establish a plan, coordination, situational analyses, evaluations, and other regulations of the information operations training, to form a strict, standardized, and unified training system, to accurately grasp the training work of the information operations, and to put it onto a standardized and legalized path. The third is that they must strengthen the training monitoring. In order to successfully implement the information operations training, they must establish an appropriate information operations coordination and supervision system, to clearly determine the responsibilities, and to specifically implement supervision and guidance over the organizational training structure of the training and of the personnel that participate. The departments that are responsible for the tasks of the supervision training pass down the training tasks, they coordinate each of the relationships between the organized training structures and the units that are participating in the training, and they urge the implementation of the training tasks, based on the unified topics, the unified steps, and the unified requirements; they delve into the training so they can genuinely guide the implementation of the training content for the units participating in the training. They promptly coordinate and

resolve each of the types of contradictions and issues that arise during the training, and they combine the training assessments. They implement effective supervision and inspection guidance for the training situations, and they practically increase the training quality.

II. They must set up a lifelike training environment and stay close to operational realities…363

The first is that they must set up "true" training environments. They must extensively use the current information operations equipment and materials **[end of page 363]**, they must fully explore the potential of the current equipment and materials, and they must adopt "live equipment simulations," "a small amount representing many," "using simulations to set up the real thing," "using the ground to represent the sea," and other measures, in order to construct lifelike information operations combat situations. They must especially focus on setting up the environment for the satellite reconnaissance, electronic interference, computer virus attacks, anti radiation attacks, psychological warfare, and other battlefield threats, which allow the training to be even better at coming close to the actual combat circumstances. The second is that they must set up "strong" combat opponents. Within the future information operations, our combat opponents, regardless of whether it is in the aspect of information operations force compilation or the weaponry functions, or of whether they are in the aspects of information operations theoretical research and tactical technology application, they are all even higher than the Chinese military. This requires that we, during the organization of the information operations training, must objectively reflect the gap between the situations of the enemy and our combat. We must not only set up the information operations technology equipment (materials) of the advanced information operations technology of the opponent, and fully reflect the information operations characteristics, but we must also reflect the other advanced operations theories and methods in a lifelike, flexible, and objective format, in the exercises, and strengthen the set up of the formidable foe. The third is that they must set up the "connection" between the forces that attend the training. The future joint campaign information operations are implemented under the joint operations background, and each type of combat force jointly implements the essentials of the information operations. The land, sea, air, space, and electromagnetic three-dimensional spaces are comprehensively developed and the air warfare, sea warfare, and land warfare are infiltrated and are jointly mixed, and the joint campaign is the fundamental support. The organization and implementation of the information operations training must adapt to the developmental trends of the joint operations, it must regard the common operations tasks as the draw, they must focus on the command, coordination, support, and war tactics of the exercises in the information operations, under the joint operations background and training topics, and enhanced the training focus.

III. They must strengthen the command capabilities training and give prominence to training on key points…364

The first is that they must strengthen the command capabilities training of the information operations commanders. The command capabilities of the information operations commanders are the concentrated reflection of the overall combat capabilities of the information operations. With regard to the guiding ideology, they must focus on the training of the complex type command personnel and troops, they must focus on the a training that is the mixture of the "command, technology, and staff," and they must fully increase the joint planning **[end of page 364]**, organized command, and information defense capabilities of the information operations commanders. With regard to the organization of the training, they must unify the planning and unify the organization. When the conditions allow, they can invite other military services to participate, and they must regard the classroom work and online training as the main organization and implementation. The second is that they must focus on various military service joint field training. They must insist upon the principles of it "being convenient for the organization and management, being convenient for the coordination of the various military services, and being convenient for the implementation and use of the communications. They must adopt the methods of unified organization and layered implementation, and they must organize the field training for each of the information operations troops (elements). When the conditions are right, they can combine the exercises and the annual training tasks, they can enhance the coordination of the navy, air force, and second artillery troops, they can implement the joint warfare and joint training of the various military service information operations, and they can genuinely research and resolve the difficulties and issues within the joint information operations. The third is that they must appropriately organize the information operations theoretical group training and online simulation trainings. During the planning work, they must make arrangements for the specialized training after the development or the specialized tactical training before the development; they must appropriately organize the information operations theoretical group training, and implement information operations theoretical training for the organizers and the backbone of participants of the information operations. Afterwards, they must fully use the current military training information networks (or command three networks) and the visual conference systems, to significantly develop the online joint exercise trainings. This type of method of intangibly using the field communications equipment does not organize the field training, its influence is relatively small, and it is easy to organize and implement in a planned way during peacetime. During the specific implementation process, they must focus on appropriately organizing the training evaluations and guaranteeing the training steps, based on the training process.

IV. They must divide the different training targets and innovate the training methods…365

During the information operations, they must adopt corresponding training methods, based on the different combat tasks and the responsibilities that each type of personnel is capable of being responsible for, in order to reach the most optimum training

results. The first is that they must divide the intelligence reconnaissance, electronic combat, network combat, psychological combat, data destruction, etc. into small groups, based on the operations tasks that they are responsible for; the second is that they must implement divisions based on the information collection, the information transmission, the information processing, the information distribution, as well as the use, and other segments of the information operations personnel; the third is that they must divide the information operations commanders and agency personnel, based on the different levels. Regardless of what principle it is based off of, implementing the division of the small groups **[end of page 365]** must be based on the different types of levels of the personnel, and the training content must have focus, in order to achieve relatively good results.

During the information operations training, they must fully use the advanced technology measures, to greatly use and create modern scientific methods, to use advanced technology results to optimize the training content and process, and to increase the quality of the information operations training. Therefore, the first is that they must carry forward the essence of the traditional training methods. The traditional training methods are the scientific method that has been combined from the long term training and its various methods are also used in the information operations training, such as the lecture methods, research and discussion methods, specialized topic methods of the theoretical study, etc. These few went through the verification of the exercises, which the traditional training methods of the scientific verification were continued to be used. The second is that they must create new training methods. The swift and violent development of the scientific technology and the continuous changes in the division of the personnel must lead to the emergence of new training methods, they must strictly follow the development of the advanced technology, they must deeply research the situations of the fundamental qualities of the information operations personnel, and they must continuously renew the training methods of the information operations training even more. For example, through the establishment of the information operations equipment training, they have the simulated and lifelike systems, they have improved the information operations theoretical study software, they have fully used the current network facilities, and they have significantly developed the online training, and other methods, which continuously increases the effectiveness of the information operations training.

This page intentionally left blank.

Chapter 22
Joint Campaign Information Operations Building…367

Joint campaign information operations (IO) building signifies the research {*yanjiu*} and preparations carried out in many respects, including operational theory, weapons and equipment {*wuqi zhuangbei*}, talent cultivation {*rencai peiyang*}, and battlefield and strength building {*zhanchang, liliang jianshe*}. This mainly includes the following: joint campaign IO theoretical research, IO weapons and equipment building, IO talent cultivation, IO battlefield construction, and IO strength building.

Section 1: Joint Campaign IO Theoretical Research…367

Joint campaign IO theory has an important guiding role {*xiandao zuoyong*} for all work of a joint campaign. It can be said that joint campaign IO theoretical preparations are the foundation of and a prerequisite {*qianti*} for all preparations for joint campaign IO.

I. Significance of joint campaign IO theoretical research…367

The practice of historical development has proven that whether military theory is advanced or not advanced influences the armed forces' prospects and victory or defeat in war. Hence, strengthening research on IO theory has important significance for seizing success in future joint campaign IO.

(1) Objective requirements {*yaoqiu*} for joint campaign IO practice

The recent several local wars have made clear that IO already has developed into an all-new **[end of page 367]** operational form {*zuozhan xingshi*}, and, speaking in a certain sense, the success or failure of IO directly influences the progress {*jincheng*} and outcome {*jieju*} of the joint campaign. It is thus clear that it is difficult for traditional operational theory to satisfy the development of joint campaign IO, which inevitably requires the guidance {*zhidao*} of new operational theory. From the viewpoint of the high ground of gaining victory in informationized war {*xinxihua zhanzheng*} and contending {*zhengduo*} in the future for our military's joint campaign information dominance {*zhixinxiquan*}, as well as the high ground of the trans-century development of unit building {*budui jianshe*}, strengthening joint campaign IO theoretical research has far-reaching real significance.

(2) Inevitable requirements for joint campaign IO strength building

Using theory to pull building is an important embodiment of bringing into play the guiding role of theory. At present, our military' joint campaign IO strength building still evinces many inadequacies. How to build the various types of strengths and on what scale they are to be activated urgently need advanced, scientific theory, conforming to

our military's reality, in order to have standards {*guifan*} and guidance. Joint campaign IO strength building involves a wide range [of issues]. It not only includes the IO unit task organization {*budui biancheng*}, but also involves the construction of the command system of systems [SoS] {*zhihui tixi*}; it not only includes the optimized combination of operational strengths, but also involves the production and application {*shengchan, yingyong*} of weapons and equipment; and it not only includes issues of the insertion of technology and funds, but also involves many real major {*zhongda*} problems such as talent cultivation. If mistakes and deviations occur in building decision-making {*jianshe juece*}, not only would there be great waste and severe losses, but it also would delay the progress of our military's joint campaign IO capabilities building. Hence, strengthening research on the major theoretical problems of our military's joint campaign IO strength building has unusually important significance for doing a good job of joint campaign IO unit building, equipment development, and talent cultivation.

(3) Needs and requirements {*xuyao*} for constructing a joint campaign IO theory SoS {*lilun tixi*}

Today, the US military has already entered the IO practice phase under IO regulations and standards {*tiaoling guifan*}. In adapting to this, our military's new-generation regulations have formally brought IO into their midst. In particular, *Chinese People's Liberation Army [CPLA] Joint Campaign Information Operations Guidelines* {*gangyao*} already regards IO as important content of a joint campaign, and has laid out standards for IO in terms of laws and regulations {*fagui*}. It is thus clear that, following on the constant development of our military's IO practice and theory, **[end of page 368]** the result is the development of joint campaign IO theory in the direction of multiple levels and the integrated whole {*duocengci, zhengtihua*}. This IO activity {*huodong*}, involving the overall situation {*quanju*} and affecting all aspects, urgently requires systematic joint campaign IO theory to serve as guidance. Constructing a joint campaign IO theory SoS, in basic theory and applied theory respects, is an enormous impetus to IO practice activity, and is an enrichment and development of joint campaign operational theory. It also is an important measure for boosting our military's joint campaign IO capabilities.

II. Main content of joint campaign IO theoretical research…369

Joint campaign IO is an all-new thing, and a good many new situations and new problems urgently await our conducting of research to resolve them. At present, joint campaign IO theoretical research must focus on basics, lay stress on application, and concentrate its efforts {下功夫 *xia gongfu*} on constructing a complete joint campaign IO theory SoS.

(1) Recognizing the joint campaign IO characteristics and laws {*tedian yu guilyu*}

Today, IO activity already has experienced a development process from low level to high level, and from practice to theory, and has composed a relatively perfect theory

SoS. However, at the joint campaign bedrock {*cengmian*}, how to recognize and grasp the characteristics and laws of IO is a new topic {*keti*} again facing us. On the future joint campaign IO battlefield, the operational means will even more tend toward the advanced; the operational modes {*zuozhan fangshi*} will be diverse; the battlefield will be highly transparent; the operational time effectiveness quality {*zuozhan shixiaoxing*} will be enhanced; the force-strength disposition {*bingli bushu*} density will decrease; command will have a high degree of adjusting-coordination {*xietiao*}; strategic-, campaign-, and tactical-level operations {*zhanlue zhanyi he zhanshuji zuozhan*} will be fused into an organic whole {*yiti*}; and the demarcation lines {*jiexian*} between the military and civilians and between the front and the rear will be blurred. Joint campaign IO's new forms, new fighting methods {*zhanfa*}, new organizational structure {*bianzhi*}, and new management and training {*xunlian*} require us to use new modes of thinking {*siwei fangshi*} to deliberate on and explore them. Researching in depth the main features {*tezheng*} of joint campaign IO, and grasping its characteristics and laws, are prerequisites for gaining success in joint campaign IO, and also are the basic foundation for IO unit building. Only by thorough research on the joint campaign IO characteristics and laws can [we] in some targeted fashion {放矢地 *fangshidi*} do a good job of the various preparations for joint campaign IO. **[end of page 369]**

(2) Exploring {*tansuo*} joint campaign IO fighting methods

Focusing on future joint campaign IO characteristics, and researching and innovating new fighting methods mutually adapted to them, are objective requirements for seizing battlefield information dominance. At present, the key points {*zhongdian*} of IO fighting methods studies are the need to mutually combine the general laws of war with the specific {*juti*} situations in our future joint campaign IO, to mutually combine them with the influence of information technology [IT] {*xinxi jishu*} on strategy and tactics, to mutually combine them with the management and social situation of the theater {*zhanqu*}, and, on the basis of scientifically analyzing the enemy and friendly sides' {*diwo shuangfang*} situation, focusing on the characteristics and development of war, and researching fighting methods conforming to and adapted to the joint campaign IO laws. Hence, in terms of research on and application of fighting methods, [we] must realize four conversions: first, in terms of the basic points of fighting methods research, is the need to convert from research on the general fighting methods of IO to joint campaign IO fighting methods research. Second, in terms of the center of gravity [COG] {重心 *zhongxin*} of fighting methods research, is the need to convert from the past special stress on carrying forward the traditional fighting methods to laying stress on researching new fighting methods such as "soft and hard integration" {*"ruanying yiti"*} and "network sabotage and severing the chain" {*"powang duanlian"*}. Third, in terms of the content of fighting methods research, is the need to convert from the past bias towards a stratagem color {*moulue secai*} in fighting methods to increasing the high-tech content of fighting methods, and realizing unity of technology and strategy {技谋合一 *jimou heyi*}. Fourth, in terms of the methods of fighting methods research, is the need to convert from the past special stress on theoretical research to a mutual combination of

theory and practice activity, such as confrontations with troops {*shibing duikang*} and simulation drills {*moni yanlian*}.

(3) Researching the applied theory of joint campaign IO

The applied theory of joint campaign IO is the critical link {*guanjian huanjie*} in the change from joint campaign IO theory to combat power {*zhandouli*}. The basic mission of applied theoretical research is to make replies to the IO principles and methods under various operational patterns {*zuozhan yangshi*}, i.e., to research the question of "what is to be done" within future joint campaign IO. Combining the reality of war development with actual research on fighting methods for the building of our military is the fundamental avenue for boosting the practicality {实用性 *shiyongxing*} of IO theory. At present, [we] must focus on the features of joint campaign IO activities {*xingdong*}, and discuss {*tantao*} how to implement IO within joint campaigns. In particular, [we] must center on the actual military struggle {*douzheng*} preparations; keep grounded in the existing organizational structure equipment {*bianzhi zhuangbei*} and its near-term possible development; and lay stress on **[end of page 370]** research on operational patterns such as the joint firepower strike campaign, island blockade campaign {*daoyu fengsuo zhanyi*}, island offensive campaign {*daoyu jingong zhanyi*}, air defense campaign {*fangkong zhanyi*}, and border defense campaign {*bianjing fangyu zhanyi*}, as well as issues such as IO characteristics and laws, operational guidance, command and coordination {*zhihui yu xietong*}, and strength application with activities to resist the powerful enemy's military intervention, so as to do a good job in the IO applied theory preparations for gaining victory in local war under informationized conditions {*xinxihua tiaojianxiade jubu zhanzheng*}.

Section 2: Joint Campaign IO Weapons and Equipment Building…371

Weapons and equipment are the material {*wuzhi*} basis for seizing victory in war. Joint campaign IO weapons and equipment building means the need to focus on the real needs and requirements of future joint campaign IO, and, in all of the preparatory work done in respects such as the development {*yanzhi*}, production, and application of weapons and equipment, to ensure the material conditions for seizing joint campaign information dominance.

I. Requirements for joint campaign IO weapons and equipment building…371

(1) Getting into shape the ideas {理清…思路 *liqing... silu*} on joint campaign IO weapons and equipment building

The characteristics of joint campaign IO determine the ideas on and development direction of weapons and equipment building. From the viewpoint of development trends, the form-state of war {*zhanzheng xingtai*} is increasingly informationized, and campaign operations also have undergone very great changes. Among them, in terms of the

operational COG, it has shifted from seeking firepower superiority as primary to seeking information superiority {*xinxi youshi*}. In terms of the operational means, it has shifted from traditional force-strength confrontation {*bingli duikang*} to confrontation with a mutual combination of "soft kill" {*"ruan shashang"*} and "hard destruction" {*"ying cuihui"*} with IO as primary. In terms of operational time and space {*zuozhan shikong*}, it has shifted from the traditional three dimensions of land, sea, and air {*lu, hai, kong sanwei*} to the land, sea, air, space, and electromagnetic [EM] multidimensional field {*lu, hai, kong, tian, dian duowei lingyu*}. The enormous changes in the form-state of joint campaign operations inevitably bring about a new transformation in IO weapons and equipment building, and also require us to adopt new ideas and modes to work out an approach {*mouhua*} to the weapons and equipment building ideas [train of thought]. At present, [we] should take the joint campaign IO characteristics as the pulling force, closely attend to the demonstration {*lunzheng*} and development {*yanzhi*} of a series of weapons and equipment for IO, **[end of page 371]** and as rapidly as possible form serialization {*xiliehua*} of the weapons and equipment. With development of IO means as a point of penetration {*tupokou*}, [we] should closely attend to the building of electronic warfare [EW] {*dianzizhan*} and network warfare {*wangluozhan*} weapons and equipment, and as rapidly as possible form weapons and equipment integration {*yitihua*}. With IO attack activities {*gongji xingdong*} as the leading factor, [we] should closely attend to the development {*yanzhi*} and production of information offense {*xinxi jingong*} equipment; and with campaign equipment as the main body, [we] should closely attend to forming IO equipment with strategic, campaign, and tactical [levels fused] into an organic whole {*zhanlue, zhanyi he zhanshu yu yiti*}, and thus boost the benefit of weapons and equipment building.

(2) Laying stress on the key points of joint campaign IO weapons and equipment building

In recent years, our military, in view of the needs and requirements of future informationized war, has built and developed a group of IO equipment with a high degree of informatization {*xinxihua chengdu*} and having our military's characteristics, and also has achieved major breakthroughs in some cutting-edge fields {*jianduan lingyu*}. However, starting out from adapting to the needs {*xuqiu*} of future joint campaign IO, these pieces of equipment are small and scattered {*xiao ersan*}, and have not formed [any] scale; this has severely restricted and influenced the generation of campaign IO capability. Hence, in order to adapt to the development trend in the application of joint campaign IO, while continuing to develop tactical IO weapons and equipment, [we] must in a manner having key points build campaign-level IO weapons and equipment. For example, "in order to sabotage {*pohuai*} the enemy's space and airborne {*kongjian, kongzhong*} strategic and campaign detection and early warning systems {*tance yujing xitong*}, [we] must energetically develop strategic and campaign information warfare [IW] weapons {*xinxizhan wuqi*} to attack the early warning satellites, early warning aircraft, and ground long-range detection and early warning radar {*dimian yuancheng tance yujing leida*}, so as to paralyze {*tanhuan*} the enemy's intelligence and reconnaissance SoS {*qingbao zhencha tixi*}, and sabotage the enemy's war preparations. In order to sabotage the enemy's command and control [C2] {*zhihui kongzhi*} and

communication systems, [we] must energetically develop space {*kongjian*} IO weapons, directed energy weapons [DEWs] {*dingxiang neng wuqi*}, and network attack weapons {*wangluo gongji wuqi*} to attack communication satellites {*tongxin weixing*} and reconnaissance, early warning, and navigation satellites, and [develop] strategic and campaign IO weapons as confrontation means to sabotage electric power systems and radio and TV systems, so as to paralyze the enemy C2 systems, and cut apart {*gelie*} the enemy operational SoS {*zuozhan tixi*}."[22] On this basis, combined with our military's **[end of page 372]** original IO weapons and equipment, [we can] form a serialized, integrated, and scalable {*guimohua*} weapons and equipment SoS adapted to joint campaign needs and requirements.

(3) Exploring models {*moshi*} for joint campaign IO weapons and equipment building

As compared to the developed nations, our military in IO weapons and equipment respects is fairly weak in the foundation, and relatively backward in technology. Thus, exploring models suited to building of our military's own weapons and equipment has important significance for reducing our military's gap with foreign militaries, and for accelerating the development of our military's IO equipment technology. At present, under circumstances where military funding {*junfei*} is limited, weapons and equipment building cannot "sow seeds on the ground" in all places {到处 "撒胡椒面" *daochu "sa hujiao mian"*}. It must persevere in leaving some things undone in order to get some things done {有所为, 有所不为 *yousuo wei, yousuo buwei*}; scientific demonstration and careful selection of projects; concentrating on the key points and sparing no effort to break through; conscientiously spurring on the integrated-whole development of our military's IO weapons and equipment SoS; truly achieving "more bang for the buck" {"少花钱, 多办事" *"shao huaqian, duo banshi"*}; and moving along a model of weapons and equipment rapid development with "fairly low investment and fairly high benefit." In terms of the building path, [we must] overcome the "hot-pursuit style" {"尾追式" *"weizhuishi"*} development model, and emphasize innovative development; in terms of the building key points, [we must] emphasize development of strategic- and campaign-level IO equipment into a SoS; and in terms of the building steps, [we must] first build the equipment urgently needed and required for actual military struggle preparations, and then develop a long-term, full set {*peitao*} of weapons and equipment. In terms of application of technology, [we must] give precedence {*youxian*} to developing critical technologies which can produce the maximum linkage [coupling] effect {*zuida liandong xiaoying*} and demonstration effect {*shifan zuoyong*}.

---

[22] Dai Qingmin {戴清民}, The Conception of Information Operations {xinxi zuozhan gainian}, PLA Publishing House, 2001, p. 356.

II. Main content of joint campaign IO weapons and equipment building…373

Under circumstances where financial resources are limited and the technology gap is fairly great, our military's joint campaign IO equipment development must emphasize taking operational needs as the pulling force; go down the path of a mutual combination of development {*yanzhi*}, importation, and transformation {*gaizao*}; within building, uphold the principle of leaving some things undone in order to get some things done; place the key points on doing well in the building of the main battle equipment for EW and network warfare; and attach importance to metasynthesis {*zonghe jicheng*} and full complements {*peitao*} of IO equipment, to gradually form an integrated {*yitihua*} IO equipment SoS with "assassin's mace" equipment {*"shashoujian" zhuangbei*} as the backbone, with third-generation equipment as the main body, with integrated network and electronic [warfare] [INEW] equipment {*wangdian yiti zhuangbei*} as the key points, with a composition of all levels {*ge cengci*} (strategic, campaign, and tactical), with mutual linkup {*xianghu xianjie*} of all services {*junzhong*}, and with integrated-whole full complements of equipment {*zhengti peitao*}. **[end of page 373]**

(1) Metasynthesis and full-complement building of IO equipment

Metasynthesis and full-complement building of IO equipment mainly means focusing on boosting systematic operational effectiveness {*xitong zuozhan xiaoneng*}; via research and development [R&D] {*yanfa*} of and allocation of area (zone) EW {*quyu dianzi duikang*} C2 systems, implementing interconnection and intercommunication {*hulian hutong*} technical transformation of IO equipment; exploiting {*kaifa*} software for intelligence processing {*qingbao chuli*}, decision-making and command {*juece zhihui*}, and management and control {*guanli kongzhi*}; and forming an IO system with the C2 system as the core, with the intelligence and reconnaissance system as assisting support {*zhiyuan*}, with the IO platforms as the main body, and with electronic information systems as the binding link {*niudai*}, to realize integration of reconnaissance and intelligence, C2, electronic attack {*dianzi jingong*}, and electronic defense {*dianzi fangyu*}. At the same time, it must strengthen the full-complement building of main battle equipment and support equipment, and of operational equipment and training equipment, to ensure as rapidly as possible helping the system to form an operational capability.[23]

(2) R&D of "assassin's mace" equipment and third-generation main battle equipment

Doing well in R&D of "assassin's mace" equipment and third-generation main battle equipment mainly involves embracing R&D of high-performance space

[23] Translator's note: unless otherwise indicated, all "support(ing)" in this chapter is "safeguarding support" {*baozhang*}.

confrontation [space warfare] {*hangtian duikang*}, satellite jamming {*weixing ganrao*}, and data link jamming {*shuju lian ganrao*} systems and integrated network and electronic" [INEW] comprehensive operational platforms; embracing development {*yanzhi*} of new-mechanism and new-concept {*xinjili, xingainian*} information weapons and equipment such as [EM] pulse bombs [E-bombs] {*maichong zhadan*}, high-performance laser weapons {*jiguang wuqi*}, and kinetic-energy anti-satellite [ASAT] weapons {*dongneng fanweixing wuqi*}; and tackling the key technical problem {*jishu gongguan*} of wireless virus attack means {*wuxian bingdu gongji shouduan*}. [This work] must boost the tactical technical characteristics {*zhanshu jishu xingneng*} of the main battle electronic equipment, including R&D of high-power, wide-frequency-domain {*pinyu kuan*}, compact, high-maneuverability {*jidong nengli qiang*} electronic jamming equipment {*dianzi ganrao zhuangbei*}, with the key points on developing airborne electronic jamming platforms {*jizai kongzhong dianzi ganrao pingtai*}, so as to boost operational effectiveness. It must apply integrated means {*zonghe shouduan*} for technical demonstration, simulation testing {*moni shiyan*}, and actual equipment testing {*shizhuang jianyan*}; strengthen real-combat testing {*shizhanhua jianyan*} of the performance of new equipment for IO; and ensure that the technology is advanced, reliable in performance, and effective in real combat.

(3) Informationized transformation {*xinxihua gaizao*} of existing weapons and equipment

Applying advanced technology to carry out informationized transformation of existing weapons and equipment is a universal practice {*zuofa*} in the refitting and generational upgrading {*gaizhuang huandai*} in armed forces of nations around the world. For example, the US military, via its practice of "putting new wine into old bottles," **[end of page 374]** carried out informationized transformation of its B-52 bombers {*hongzhaji*} and preserved the advanced quality of their performance, precisely a case in point. Our military, in terms of a specific avenue for carrying out advanced technical transformation of existing IO equipment, can adopt the method of a mutual combination of internal embedding {内部嵌入 *neibu qianru*} and external integration {*waibu jicheng*}. By embedding and fusing IT, or adding information devices to carry out transformation and replacement of some components {*bujian*} of existing single pieces of weapons and equipment, their performance is improved. By exploiting IT and horizontal integration {*hengxiang yitihua*} technology to carry out metasynthesis of originally discrete existing weapons and equipment or systems, the operational capability of weapons and equipment is boosted.

Section 3: Joint Campaign IO Talent Cultivation…375

Faced with the severe challenges of the worldwide new military transformation, our military must fulfill the historic missions of building informationized armed forces and gaining victory in informationized war; but without a large group of high-quality joint campaign IO talent, this is a fundamentally impossible task. Hence, we must regard the cultivation and training {*zaojiu*} of a large and high-quality joint campaign IO talent

contingent as a matter of fundamental importance {根本大计 *genben daji*} for armed forces modernization, and place it in a prominent position.

I. Talent needs for joint campaign IO…375

Joint campaign IO talent signifies military talent adapted to the requirements of gaining victory in informationized war and to organizing and commanding joint campaign IO activities. It means high-quality servicemen {*junren*} having good information accomplishments. IO talent must possess excellent political quality, military quality passing the stiffest test, solid cultural quality, and strong and healthy physical and mental quality. At the same time, it also should have information quality conforming to the requirements of the Information Age, and embodying the essential characteristics of talent in the military information field. For the present time, [we] should lay stress on cultivation of the following three types of talent: **[end of page 375]**

(1) IO command talent

IO command talent includes two aspects: the first is IO command talent and the second is joint operations command talent. In order to adapt to the needs and requirements of joint campaign IO, IO commanders {*zhihuiyuan*} not only must understand command tenets, command procedures {*zhihui chengxu*}, command content, and command modes {*zhihui fangshi*}, but also must be proficient in the operation and use {*caozuo shiyong*} of various advanced command tools, and possess very strong man-machine conversation [dialog] {*ren—ji duihua*} capability. As an important component {*zucheng bufen*} of joint campaigns, IO will penetrate from the start to the finish of operations. This then requires that the joint campaign commander be able to focus on the joint campaign IO characteristics; have the capability to apply multiple avenues to acquire information, full-dimensional information processing capability {*quanfangwei xinxi chuli nengli*}, and the capability to exploit information networks to command IO activities, as well as the capability to mount swift responses to new information and to complex battlefield environments; and be able to occupy [the high ground of] the joint campaign's overall situation to macroscopically work out an approach in planning {*hongguan mouhua*} of the IO activities.

(2) IO staff officer talent {*canmou rencai*}

IO staff officer talent is the group {*qunti*} which assists the IO commander in command decision-making {*zhihui juece*}. Staff personnel must have profound IO professional knowledge {*zhuanye zhishi*} and extensive correlated knowledge as a supplemental structure of knowledge {*buchongde zhishi jiegou*}. Within operations, they [must] be able to skillfully apply computers to analyze terrain; be able to use positioning systems to position and navigate; be able to interpret {*pandu*} and analyze various types of photographs, including aviation and satellite photos; and be able to read the main operational opponent's military maps. They [must] be able to skillfully use computer and network technology {*jisuanji he wangluo jishu*} to search for and manage various types

of data resources, and be able to skillfully use computers to perform scientific, rapid calculations and draft {*nizhi*} military documents. At the same time, they must have fairly strong analysis and assessment {*fenxi panduan*} capability, the capability for working out an approach in planning using mathematical and scientific methods {*yunchou mouhua*}, the capability for organization and adjusting-coordination, inspection and guidance {*jiancha zhidao*} capability, and research and innovation {*yanjiu chuangxin*} capability, to assist the senior officer {*shouzhang*} in setting the resolution {*dingxia juexin*} and realizing the resolution, and creatively launching {*kaizhan*} the work.

(3) IO combat talent

IO combat talent mainly signifies IO combat operating personnel {*zhandou caozuo renyuan*}. As combat personnel, they [must] have the ability to exploit many types of reconnaissance and detection equipment and means {*zhencha tance zhuangbei he shouduan*}, **[end of page 376]** to swiftly and accurately ascertain the enemy intent {*yitu*}, and to properly carry out the preparations for executing IO attacks; be able to synthetically apply {*zonghe yunyong*} IO equipment and exploit computer knowledge to carry out attacks on and sabotage of enemy information systems, and paralyze the enemy's command information systems; grasp multilayer defense {*duoceng fangyu*} means to guard against sabotage by computer viruses {*jisuanji bingdu*} and intrusions by computer hackers {*heike*}; and be able to rapidly restore software and hardware which have suffered enemy sabotage.

II. Talent cultivation modes for joint campaign IO…377

Joint campaign IO talent cultivation not only has points in common with cultivation of general operational talent, but also has its own special quality {*teshuxing*} of cultivation. Hence, in terms of cultivation modes, the "main channel" role of cultivation at military colleges and schools {*yuanxiao*} inevitably will be brought into play. At the same time, relying on the superiority of national education to have specially emphasized cultivation of the associated professional talent, on this basis [we] also must employ multiple modes and avenues, including continuing education, short-term training, and advanced studies abroad {出国深造 *chuguo shenzao*}, to increase the cultivation's degree of force {*lidu*}, and do everything possible to both ably and rapidly cultivate talent adapted to joint campaign IO needs and requirements. Right now, [we] must, based on the needs and characteristics of IO talent, implement the cultivation in a planned manner having a directed [focused] quality {*you jihua, you zhenduixing di*}.

(1) Enhancing the directed [focused] quality of the military college and school cultivation of IO talent

The diversity of joint campaign IO talent has determined the complexity and arduousness of military college and school cultivation of it. In focusing on cultivating high-quality joint campaign IO talent, the pressing matter of the moment {当务之急

dangwu zhiji} is the need to realize the "three transformations" {*"sange zhuanbian"*} in armed forces college and school talent cultivation. The first is the transformation from a single-structure model to a composite-structure model {复合结构型 *fuhe jiegou xing*}. The development trend of modern scientific integration {*zonghehua*}, technological integration {*jichenghua*}, and knowledge diversification, and the wide-ranging employment of digitized units {*shuzihua budui*} and precision guided munitions [PGMs] {*jingque zhidao wuqi*} on the future informationized battlefield are causing unit building to tend toward combinedness {*hechenghua*}. If the experience of IO personnel is unitary and simple, they will have difficulty in adapting to joint campaign needs and requirements under informationized conditions. [We] should focus on new knowledge, new equipment, new technologies, and new fighting methods, to realize recombination {*fuhe*} of military command, political work, and logistics {*houqin*} and equipment support; recombination of command, management, and technology; and recombination of academic research and military application. Second is **[end of page 377]** the transformation from knowledge-model education to capabilities-model education. In the past, vis-à-vis the cultivation of talent, we laid relative stress on the imparting and instilling of knowledge, and the quality structure of the cultivated talent was relatively unitary; the capability for receiving high/new-tech knowledge {*gaoxinkeji zhishi*} and the capability for adapting to unit needs and requirements were both fairly poor, and lacking in staying power and development potential. The cultivation of IO talent should lay stress on boosting their comprehensive quality, and, in the transformation from "knowledge-model education" to "capabilities-model education," constantly enhance their adaptability {*shiying nengli*}, innovative capability, and follow-up development potential. Third is the transformation from classroom theoretical teaching as primary to theory plus practice. The traditional classroom teaching model {*moshi*} has a simple and dry form, and its cultivation and training {*peixun*} quality is not high. [We] should, on the basis of classroom theoretical teaching, fully bring into play the integrated superiority {*zonghe youshi*} of the colleges and schools, units, and scientific research institutions {*keyan jigou*}; strengthen exchanges; establish cooperative relationships for jointly cultivating talent; and form integrated-whole composite strength {*zhengti heli*}, [all of which] has important significance for the cultivation of IO talent. In this way, [we] not only bring into play their respective superiorities, but also enable the [above] three to boost and promote one another. In other words, [we] thus have boosted the cultivation quality and benefit of the IO talent, and also have provided unit building with technical services, information services, and talent services. The colleges and schools should, via planned-manner organizing of students to travel to the units for investigation {*diaoyan*}, field work {实习 *shixi*}, and substitute duties {代职 *daizhi*}, take initiative to understand the requirements of future IO for talent quality, and to understand the knowledge and capabilities needed for holding posts. In particular, they must understand the new equipment development trends and the realities of unit training methods {*xunfa*} and fighting methods reform, to provide talent and technical support {*zhichi*} for their scientific research and training.

(2) Broadening the approaches to national education's cultivation of IO talent

The cultivation of IO talent not only has its own special quality, but also has a good many common qualities {*gonggongxing*} and points of interlinking {相通之处 *xiangtong zhichu*} with the cultivation of socially informationized talent. A good many nations around the world have already gone along this approach of relying on national education to cultivate IO talent. Within UNESCO's world science report for 1996, it was made known that the U.S. had more than 780,000 scientists directly and indirectly in service to the military, and that this accounted for 82% of all American scientists. Every year since 1980, the US military has had almost 45% of its newly **[end of page 378]** commissioned officers directly taken from local colleges and schools. The British military's newly commissioned officers basically all have locally received a higher education, and the UK's 44 regular military colleges and schools mainly undertake training missions before officer posting or before promotion. The information-field discipline in China's local colleges and universities has very powerful real strength in running teaching programs {*banxue shili*}; moreover, the various disciplinal professions are complete, the curriculum SoS is perfect, the qualified teacher strengths are abundant, the teaching facilities equipment {*shebei*} is advanced, and the information sources are wide-ranging. It can be said that they are the "mother lode" {*"fukuang qu"*} for all types of information combat talent {*xinxi zhandou rencai*}. Hence, [we] must, based on the cultivation objectives {*mubiao*}, constantly increase the cultivation degree of force, and truly tap the superiority of social information resources for our purposes.

(3) Strengthening the mechanisms {*jizhi*} for continuing education's cultivation of IO talent

Under circumstances where the renewal speed of current knowledge is growing ever faster, knowledge in terms of each person always has a problem of attenuation. Statistics show that in the early period of the 20th century, knowledge worldwide doubled every 10 years, but by the 1970s, it was doubling every 5 years, and today the half-life period {*banshuai qi*} of knowledge is roughly 2-3 years. Especially in the information discipline's professional fields {*zhuanye lingyu*}, following on the full-speed development of IT, the "depreciation" {*"zhejiu"*} of technical knowledge is even more rapid. This requires strengthening of continuing education mechanisms; increasing continuing education's degree of force; and via multiple avenues. continuing education, short-term cultivation and training, assembling for training {*jixun*}, sending off for schooling and rotational training {送学轮训 *songxue lunxun*}, and substitute-duty accompanied training {代职随训 *daizhi suixun*}, implementing a system {*zhidu*} of duty cultivation and training {*renzhi peixun*} and post cultivation and training {*gangwei peixun*} for all types of personnel in IO, accelerating the implementing of the plan for IO talent to strengthen the army {*xinxi zuozhan rencai qiangjun jihua*}, seeing that continuing education goes along a normalized and systematized track {*zhengguihua, zhiduhua guidao*}, helping the IO talent to constantly renew their structure of knowledge, and precipitating the fission {*liebian*} and breeding of knowledge.

Section 4: Joint Campaign IO Battlefield Building [Construction]…379

Joint campaign IO battlefield building signifies the various types of preparatory work done in peacetime order to meet joint campaign **[end of page 379]** IO needs, in respects such as the IO battlefield essential factors {*yaosu*}, the battlefield management system {*guanli tizhi*}, and battlefield protection. In terms of a relatively perfect traditional battlefield infrastructure building {*jichu sheshi jianshe*}, IO battlefield building is a new field under informationized conditions, and also is the basis for wartime seizing of success in joint campaign IO.

I. Objectives of joint campaign IO battlefield building…380

The IO battlefield is the entire multidimensional battlespace {*duowei zhanchang kongjian*} which takes IT as its foundation, which takes the information environment as its backing, which takes IO weapons and equipment and battlefield information networks as support {*zhicheng*}, and which can realize sharing {*gongxiang*} of all types of information resources and real-time switching of IO, to support {*zhichi*} the IO activity of command personnel, operational personnel, and operational support personnel. Joint campaign IO battlefield building, besides construction of the traditional battlefield installations {*sheshi*}, also should place the key points on doing well in the following several respects.

(1) Timely shared information resources bases {*xinxi ziyuanku*}

Battlefield information resources building is an important basis for joint campaign IO, and is an inevitable requirement for boosting the IO benefit. To focus on the joint campaign IO requirements, information resources building must lay stress on building in the aspects of informationized map bases {*xinxihua dituku*}, weapons and equipment resources bases {*wuqi zhuangbei ziyuanku*}, and intelligence resources bases {*qingbao ziyuanku*}. Informationized maps signify, within a predetermined battlefield scope, maps/charts of the operational geographic information essential factors which meet the needs and requirements of the joint campaign IO commander and his command organ {*zhihui jiguan*}. These maps are required to be precise {*jingque*}, simple and convenient, and full and accurate in content. The weapons and equipment resources base is composed of essential factors such as the enemy and friendly sides' main IO weapons and equipment tactical and technical characteristics {*zhanshu, jishu xingneng*} and their application requirements, and is one of the foundations for the commander and his command organ to command the operations. The intelligence resources base signifies, via establishing of a complete, accurate, and detailed intelligence information database {*qingbao xinxi shujuku*}, the basis supplied for the operational decision-making of the commander and his command organ.

(2) Interconnected and intercommunicating {*hulian, hutong*} battlefield information networks

Battlefield information networks are the foundation for the open-up development and exploitation {*kaifa liyong*} of battlefield information resources and for IT application, and are important means for information transmission, switching, and sharing. Battlefield information networks **[end of page 380]** mainly include two large classes {*lei*}, shared information networks {*gongyong xinxi wanguo*} and dedicated information networks {*zhuanyong xinxi wangluo*}, and are the main-body essential factors of informationized battlefield building. In order to meet our military's joint campaign IO requirements, the near-term development objectives for battlefield information network building are as follows: the first is to enlarge the battlefield information network coverage scope, so that it can cover all operational units {*zuozhan budui*} and organs, as well as all preset battlefields, and radiate to all operational elements {*zuozhan danyuan*}, thus composing the basic backing for the IO battlefield. Second is to enhance the information networks' battlefield adaptability, to ensure uninterrupted command {*bujianduande zhihui*}. Third is the need during building to apply advanced, mature technologies to realize real-time transmission of multiple types of information, including voice, data, and imagery, and provide users with a variety of convenient functions. Fourth is boosting security and secrecy {*anquan baomi*} and protection capability.

(3) A standardized, integrated {*biaozhunhua, yitihua*} battlefield SoS

The standardized, integrated battlefield SoS not only is a requirement for technical design {*jishu sheji*} and application, but also is an inevitable requirement for the joint campaign IO battlefield SoS. Within it, standardization is the "bottleneck" restricting the integration of information systems and the information flow volume and flow speed, and is the key to realizing intercommunication and interconnection among all systems and all elements on the battlefield. Integration means the integration realized for information systems on the battlefield, including early warning and detection, intelligence and reconnaissance, C2, and EW; the integration realized for battlefield information collection, transmission, and processing; and the vertical and horizontal integration {*zongxiang he hengxiang yitihua*} realized for all operational elements and all operational systems. A standardized, integrated battlefield SoS is an assurance for boosting battlefield survivability {*shengcun nengli*} and combat power.

II. Main content of joint campaign IO battlefield building…381

The main content of IO battlefield building includes IO battlefield management SoS building, building of the IO battlefield's basic essential factors, battlefield information network construction, protective engineering {*fanghu gongcheng*} construction for battlefield information installations, construction of battlefield information management and control installations {*xinxi guanzhi sheshi*}, and open-up

development and reserve {*kaifa yu chubei*} of battlefield information resources. **[end of page 381]**

(1) Building of the IO battlefield management SoS

IO battlefield management SoS building mainly includes the following several aspects: the first is managing and organizing the SoS building. In order to adapt to the needs and requirements of IO battlefield management work, the theater should establish an IO battlefield building management institution, responsible for the IO battlefield management work related to all systems in that theater. Second is the building of the management systems and means. [We] must exploit advanced management technology to establish an automated management system {*zidonghua guanli xitong*}, in order to realize effective management and to enhance management levels {*shuiping*} and capability. Third is the building of management policy laws and regulations {*zhengce fagui*}. [We] must formulate the corresponding full set of policy laws and regulations, to facilitate applying all available battlefield information resources, and to assure information sharing and normal order {*zhixu*}. Fourth is the building of a management index SoS {*zhibiao tixi*}. Based on the needs and requirements for IO battlefield building and management, the establishing of specific tactical and technical management indexes is an objective requirement for assuring the rapid adjusted-coordinated development of the IO battlefield work.

(2) Building of the basic essential factors of the IO battlefield

The IO battlefield's basic essential factors are mainly embodied in six respects. First are the basic essential factors of information collection {*caiji*}. These mainly include observation and communication radar stations {*guantong leidazhan*}, sonar reconnaissance stations {*shengna zhenchazhan*}, communication reconnaissance and detection stations {*tongxin zhencezhan*}, medium/long-range direction finding stations {*zhongyuanjuli cexiangzhan*}, phased array radar stations {*xiangkongzhen leidazhan*}, and trajectory-measurement phased array radar stations {*dandao celiang xiangkongzhen leidazhan*}. Second are the basic essential factors of information transmission. These mainly include various types of fixed communication stations, hub node stations {*shuniu jiedianzhan*}, satellite ground stations {*weixing dimianzhan*}, and various types of mobile base stations {*yidong jizhan*}. Third are the basic essential factors of information processing. These mainly include information processing centers composed of hardware platforms and software systems. Fourth are the basic essential factors of IW {*xinxi duikang*}. These mainly include transceiver jamming stations {*diantai ganraozhan*}, radar jamming stations {*leida ganraozhan*}, and space satellite jamming stations {*kongjian weixing ganraozhan*}. Fifth are the basic essential factors of information control. These mainly include C2 centers at all levels. Sixth are the basic essential factors of information support. These mainly signify monitoring facilities equipment {*jiankong shebei*}, air and temperature regulation facilities equipment, and all types of service {*qinwu*} support installations. **[end of page 382]**

(3) Battlefield information network construction

Battlefield information networks are integrated {*yitihua*} battlefield information nets with military-use and public information communication nets {*junyong gonggong xinxi tongxin wang*} as the basis, forming system-of-nets integration {网系集成 *wangxi jicheng*}, and [having] security and secrecy {*anquan baomi*} and flexibility {*jidong linghuo*}. In this system-of-nets structure {*wangxi jiegou*}, the unified node structural form and functional positioning {*gongneng peizhi*}, and the positioning of essential factors for a unified standard {*tongyi guifan*} "user application net + marginal net {*bianyuan wang*} + core net" [together] realize seamless interconnection {*wufengxi lianjie*} of fixed information communication nets and mobile {*jidong*} information communication nets, strategic information communication nets and campaign/tactical information communication nets, public information communication nets and service and service arm {*junbingzhong*} dedicated information communication nets, and military information communication nets and civilian information communication nets. In terms of the relationship of communication to the command information systems and weapons systems, they realize metasynthesis. In terms of the technical system {*tizhi*}, they realize technical system unification of the common equipment {*gongxing zhuangbei*} of all services and arms. In terms of services {*yewu*}, they integrate support {*zonghe zhichi*} for voice, data, imagery, and multimedia services. In terms of network control and management, they realize automation, smartness {*zhinenghua*}, and synthesis {*zonghehua*}. In terms of network security and secrecy {*wangluo anquan yu baomi*}, they realize multilevel security, multilevel secrecy, and synthesis into an organic whole {*zonghe yiti*}. In terms of organization and application, they support {*zhichi*} dynamic reorganization {*dongtai chongzu*}, and have both independent application and synthetic application.

(4) Protective engineering construction for battlefield information installations

Within future operations, information installations will be the targets of first choice for enemy strikes. Hence, during building [we] must, based on the information installations' protection requirements, adopt protective engineering construction mutually adapted to them. Within this, important installations such as C2 centers, communication centers, and data processing centers should be built underground or in cave depots {*dongku*}; generator rooms or workstations {*gongzuozhan*} having EM radiation {*dianci fushe*} must during building have shielding materials {*pingbi cailiao*} installed in their surrounding walls, to prevent EM leakage {*dianci xielou*}; information installations undertaking important missions can carry out double-address backup {双址备份 *shuangzhi beifen*} or bistatic [dual-base] construction {*shuangjidi jianshe*}; and information installation construction on the ground should comprehensively consider protective camouflage {*weizhuang*}, so as to boost wartime survivability.

(5) Battlefield information management and control installation construction

Battlefield information management and control installation construction mainly signifies battlefield spectrum management and control {*pinpu guanzhi*} installation construction, **[end of page 383]** information management and control station {*guanli kongzhi taizhan*} construction, and building of information management and control means and systems. Within these, a spectrum-resources comprehensive {*zonghe*} management system is the key point for battlefield information management and control building. The spectrum-resources comprehensive management system should combine into an organic whole the functions of radio/wireless signal monitoring {信号监测 *xinhao jiance*}, positioning, analysis and frequency allocation {*pinlyu fenpei*}, and real-time indication and allocation {指配 *zhipei*}.

(6) Battlefield information resources open-up development {*kaifa*} and reserve

The open-up development of information resources must be carried out under a unified technical system {*tizhi*} and standards system {*biaozhun tizhi*}; this is the foundation for realizing information resources exploitation and sharing {*liyong he gongxiang*}. Our military's information resources in overall terms can be divided into shared information resources and special-purpose information resources. Shared information resources signify the shared information resources providable to the three services, while special-purpose information resources signify information resources correlated only to one unit {*danwei*} or system service {*xitong yewu*}. Shared information resources should be given unified organization and open-up development, while special-purpose information resources are organized and open-up developed by the employing unit {*shiyong danwei*}. The open-up development of information resources is the critical link in boosting the data and quality of the information resources. It mainly should be carried out by centering on several links: information resources collection, information resources tapping {*wajue*}, and information resources optimized regeneration {*youhua zaisheng*}.

The reserve of information resources is the use of certain methods to store the achievements of the open-up development of information resources, to facilitate the ability to timely exploit them when needed and required. Reserve of information resources is mainly realized via the mode of class-by-class establishment {*fenlei jianli*} of databases and their management systems [DBMSs].

Section 5: Joint Campaign IO Strength Building…384

The IO strengths are the main body for implementing joint campaign IO, and are the keys to bringing into play IO technical equipment effectiveness and to boosting IO capability. Joint campaign IO strength building must focus on boosting IO capability, fully bring into play the tactical and technical characteristics of the IO weapons and equipment, take the acquisition of battlefield information superiority **[end of page 384]** as the pulling force, and, on the basis of the existing IO units, step up reform and

perfection, and strive within a fairly short time to build them into a force structure {*liliang jiegou*} and scale adapted to future joint campaign IO needs and requirements.

I. Requirements for joint campaign IO strength building…385

IO strength building must take the joint campaign IO battlefield needs and requirements as the criteria {*zhunze*}, to achieve the basic objectives of high command efficiency {*zhihui xiaolyu*} and strong comprehensive operational capability {*zonghe zuozhan nengli*}.

(1) Being elite, highly efficient, and moderate in scale {*jinggan, gaoxiao, guimo shidu*}

The joint campaign IO activities confrontation {*xingdong duikang*} is sharp and technology intensive {*jishu miji*}, and its implementation degree of difficulty {*shishi nandu*} is high. Hence, being elite, highly efficient, and moderate in scale has become a general requirement {*zongti yaoqiu*} for IO strength building. First of all is conformance with China's actual economic real strength foundation. Since all types of IO weapons and equipment within IO unit equipment are highly technology intensive, their funding investment is enormous, and large amounts of capital {*zijin*} are invested within a fairly short time to build IO strengths on a huge scale. This not only is unrealistic, it is also unnecessary. [We] must move along a building approach of economic practicality. Next is being beneficial to boosting of battlefield survivability. In future joint campaign IO, the confronting sides {*duikang shuangfang*} will in large quantities apply high-grade, precision, and advanced {高, 精, 尖 *gao, jing, jian*} weapons and equipment; battlefield transparency will be increased, and lethality {*shashangli*} and destructive power {*pohuaili*} will be sharply increased; and the threats to large-scale units moreover will grow ever higher. Hence, elite, highly efficient, moderate-sized IO units are becoming the development trend. Third is conformance to the characteristics of IO activities. Joint campaign IO mainly is a confrontation in the EM field and in the network field, and its prominent characteristics are a strong technical quality and non-contact operations {*feijiechu zuozhan*}. Hence, building an IO strength [contingent] with a high S&T content and moderate scale is an inevitable requirement for carrying out IO missions.

(2) Facilitating implementation of high-efficiency joint campaign IO command

Joint campaign IO strength building must take boosting of IO command benefit as a basic requirement. This is because, on one hand, the IO battlefield scope is expansive, and battlefield situations change rapidly, objectively requiring that the commander and his command organ must **[end of page 385]** accelerate command speed and boost command efficiency, so as to effectively command and control the IO units. On the other hand, the IO weapons and equipment technological confrontation is pronounced, opportunities for combat {*zhanji*} are fleeting {瞬间即逝 *shunjian jishi*}, and some situations are even difficult to anticipate. Hence, this subjectively requires that the commander and his command organ must be highly efficient in command, so as to adapt

to the situation of IO battlefield changes. In addition, boosting command efficiency in terms of the integrated whole, and enhancing battlefield adjustment-control capability {*tiaokong nengli*}, also are basic requirements of future joint campaign IO.

(3) Being beneficial to bringing into play IO weapons and equipment effectiveness

Joint campaign IO strength building involves many aspects, including the strength scale and its system and organizational structure {*tizhi bianzhi*}. Among these, technical equipment also is an indispensable aspect. From the viewpoint of the development of IO practice, it mainly is composed of EW and network warfare; and the EW strengths and network warfare strengths are the main body of the IO strengths. In other words, EW equipment and network warfare equipment are the main-body parts of the IO equipment. However, the above weapons and equipment not only are mutually different in performance, but also are greatly dissimilar in operational application. For example, EW equipment, from the viewpoint of operational disposition {*zuozhan bushu*}, not only can be dispositioned on the ground, in the air, and at sea, but also can be [deployed] in outer space {*taikong kongjian*}. From the viewpoint of jamming operating distance {*ganrao zuoyong juli*}, some of it is long-distance jamming equipment, and some is short-distance jamming equipment; and from the viewpoint of jamming technology, some of this equipment is for communication jamming, and some is for radar jamming, etc. Hence, bringing into play to the maximum extent the technological superiority of the IO weapons and equipment, and optimally combining the weapons and equipment integrated-whole strength, are inevitable requirements of IO strength building.

II. Ideas on [train of thought in] joint campaign IO strength building…386

The building of joint campaign IO strengths is a new thing. We should take as the foundation the successful experiences of the past few years of strength building; be grounded in the present; focus on the future; and explore a path to success which is economical, highly efficient, and suited to China's national conditions and military conditions. **[end of page 386]**

(1) Laying stress on the key point of campaign-level IO strength building

The campaign-level IO strengths are the main body for carrying out the joint campaign IO missions, and within all IO strength building they are in the leading position {*zhudao diwei*}. At present, our military's IO strengths mainly are composed of IO strengths at three levels: strategic, campaign, and tactical. The technical equipment and operational application of the various types of strength are mutually different; moreover, the tactical-level IO unit scale is fairly large, leading to imbalance in the integrated-whole force structure {*zhengti liliang jiegou*}. From the viewpoint of the actual situation, the development speed of the campaign-level IO strengths is fairly slow, and their structure is not exactly reasonable {不尽合理 *bujin heli*}; they are far from being able to adapt to joint campaign IO needs. Hence, within the building process, [we] must tightly

concentrate on this key point, viz., campaign IO strength building; scientifically demonstrate it from the aspects of talent cultivation, equipment needs, and unit structure; take the two types of main-body strengths, EW and network warfare, as the pulling force; and, by optimizing the internal force structure, accelerate the steps to IO strength building.

(2) Reforming and adjusting the current IO force structure

At present, our military's IO strengths are developing from the original assisting support and safeguarding support {*zhiyuan baozhang*} strengths into important operational strengths, and the speed and scale of strength building are correspondingly increasing. However, from the viewpoint of the integrated whole of our military's present IO strengths, still present are phenomena such as the structural hierarchy {*jiegou cengci*} being not exactly reasonable, fairly large divergence in technical equipment, and developmental imbalance in the various services' strengths. For example, the Army {*lujun*} EW strengths already have formed a certain scale, but most of its weapons and equipment are at the tactical level; and the Navy and Air Force EW strengths have somewhat developed, but their development speed and scale still cannot meet operational needs and requirements. Hence, [we] must concentrate efforts on resolving the existing problems; take adapting to future joint campaign IO needs as the objective; reform the existing unit structural hierarchy; step up R&D and demonstration of technical equipment; adjust the distribution {*buju*} and composition of IO strengths among all services; and do everything possible within a fairly short time to build them into a [contingent of] IO units with a balanced development of service strengths, with fairly advanced equipment, and with adaptation to future operational needs and requirements. **[end of page 387]**

(3) Strengthening training, boosting comprehensive operational capability

Boosting comprehensive operational capability is the basic objective in IO strength building. If [we] want to accomplish this point, besides having a scientific and rational organizational structure and system {*bianzhi tizhi*}, command relationships {*zhihui guanxi*} which are smooth and ordered {*shunchang youxu*}, and advanced battlefield information networks, [we] also need to have the units undergo long-term, large-volume training and practice activity {*xunlian shijian huodong*}. IO unit training mainly sets about in the following several respects: the first is laying stress on unit training under complex EM environments. In future informationized operations, the battlefield will have large quantities of electronic facilities equipment of different frequency bands {*pinduan*} and different systems {*tizhi*}; moreover, their multitude of quantities and high density will create very great influences on unit operational activities {*budui zuozhan xingdong*}. Added to this, the IO weapons and equipment per se will have large quantities of electronic information facilities equipment. How to properly handle the application relationships among the various types of information facilities equipment, and bring into play the superiority of the IO weapons and equipment's own performance, thus will require going through peacetime setup {*shezhi*} of complex EM

environments, seeking within training the laws {*guilyu*} of IT equipment application, and enhancing the directed [focused] quality of IO training. Second is laying stress on joint training {*lianhe xunlian*}. On one hand, [we] must emphasize jointness between the IO units and the other units, discover inadequacies within the training process, find disparities/gaps {*chaju*}, and thus form integrated-whole operational capability. On the other hand, [we] must emphasize jointness among the internal strengths of the IO units, and conduct training activity to enhance the coordination capability among their own internal strengths, among the weapons and equipment, and within application of the different means, to boost the IO's own operational capability. Third is applying simulation means {*moni shouduan*} to boost the training benefit. From the viewpoint of the main practices of foreign militaries, the method of a mutual combination of combat simulation [war games] {*zuozhan moni*} and exercises {*yanxi*} is an effective avenue for boosting unit training quality. Practice has proven that application of simulation technology can in a lifelike manner reproduce a variety of battlefield environments and, after introducing various variables and essential factors {*bianliang yaosu*}, rapidly display the situations of various training results. Also, within complex EM environments, [we] can apply composite simulators {*fuheshi moniqi*} to carry out simulation testing {*moni jianyan*} of various types of weapons and equipment undergoing new open-up development. Via scientific simulation and emulation means {*moni fangzhen shouduan*}, [we] maximally promote the joint campaign IO units' training quality, and boost their training levels. **[end of page 388; end of chapter]**

Chapter 23
U.S. and Taiwan Information Operations…389

The U.S. and Taiwan militaries both attach extreme importance to the role {*zuoyong*} of information operations [IO] within modern war, and have made very great efforts in the research {*yanjiu*} aspects of IO. Moreover, they have also realized very good achievements.

Section 1: Information Operations of the US Military…389

The US military holds that modern war is now developing precisely in the direction of taking the seizure of information superiority {*xinxi youshi*} as primary, that IO already has become an all-new operational pattern {*zuozhan yangshi*}, and that the influence which IO will produce on modern war will be greater than that of any one operational pattern of the past. At the same time, it emphasizes that in future wars, the seizure of information superiority will be the fundamental assurance of seizure of all-around military superiority, and will be a basic prerequisite {*qianti*} for winning wars; and it has applied this thought within several recent local wars. No matter whether in the Persian Gulf War {*haiwan zhanzheng*} of the early 1990s or in the later Kosovo War and Iraq War, the US military has always attached the fullest importance to applying an organic combination of IO and other operational activities {*zuozhan xingdong*}, and has elevated IO activities to the strategic high ground of awareness. Also, it is precisely the fact that it has this rich war practice as a support {*zhicheng*} and testing {*jianyan*} [ground] which has enabled the US military's awareness of IO to become ever deeper; [its] IO capability is constantly increasing, and it has formed a relatively complete IO theory. **[end of page 389]**

I. Basic viewpoints and principles of US military IO…390

The US military holds that the essence of IO is to use information capability {*xinxi neng*} as the main functional means {*zuoyong shouduan*}, and use "information flow" {*"xinxi liu"*} to control "capabilities flow" {*"nengliang liu"*} and "material flow" [logistics] {*"wuzhi liu"*}, so as to usurp {*buduo*} the enemy's decision-making capability {*juece nengli*} and preserve friendly {*jifang*} decision-making superiority {*juece youshi*}, and, via ultimate attacks on the enemy's understanding {*renshi*} and conviction, to force the enemy to drop his resistance {*fangqi duikang*}.

IO has broad-sense and narrow-sense parts. Broad-sense IO signifies the confrontation {*duikang*} and struggle {*douzheng*} conducted by the opposing sides {*didui shuangfang*} in the political, economic, science and technology [S&T] {*keji*}, diplomatic, cultural, and military fields {*lingyu*}, as well as on the battlefield, and exploiting information technology [IT] {*xinxi jishu*} means to contend for information superiority. Broad-sense IO is divided into two types: wartime and peacetime. Narrow-sense IO signifies "battlefield information warfare [IW] {*xinxizhan*}" or "command and

control [C2] warfare" {*"zhihui kongzhizhan"*}. This indicates, under intelligence assisting support {*qingbao zhiyuan*}, using multiple means, entity destruction {*shiti cuihui*}, electronic warfare [EW] {*dianzizhan*}, military deception [MILDEC] {*junshi qipian*}, operations security [OPSEC] {*zuozhan baomi*}, and psychological operations [PSYOP] {*xinlizhan*}, to attack the enemy's entire information system {*xinxi xitong*}, and disrupt {*pohuai*} or sever the enemy information flow, so as to influence, weaken, or destroy the enemy's command information system capability, and at the same time protect friendly command information system capability. [Translator's note: in this section only, due to US military usage, all "support(ing)" unless otherwise indicated is "assisting support" {*zhiyuan*}.]

(1) Basic viewpoints

1. Seizing battlefield decision-making superiority is the basic goal {*mudi*} of IO.

The joint *Information Operations* regulations {*lianhe xinxi zuozhan tiaoling*} [joint] publication [JP 3-13] by the US military in 2006 clearly points out the following: "Information operations (IO) are described as the integrated employment {*zonghe liyong*} of electronic warfare (EW), computer network operations (CNO) {*jisuanji wangluozhan*}, psychological operation (PSYOP), military deception (MILDEC), and operations security (OPSEC) [as the core capabilities], in concert {*peihe*} with specified {*teding*} supporting and related capabilities, to influence, disrupt {*pohuai*}, corrupt {*raoluan*}, or usurp adversarial human and automated decision making while protecting our own."[24] In other words, the main objective {*mubiao*} in the US military's implementation of IO is to usurp the adversary's decision-making capability, and the fundamental goal which must be achieved is to seize decision-making superiority. This is significantly different from the viewpoint of the 1998 joint *Information Operations* regulations [also called JP 3-13], so that its understanding was constantly deepening. In the 1998 version of joint *Information Operations* regulations, the US military had held that "information operations are activities to influence the enemy's information and **[end of page 390]** information systems, while protecting friendly information and information systems," and that their fundamental goal was "to seize information superiority." This [change] from "information superiority" to "decision-making superiority" in reality was the elevation of IO from the campaign level {*zhanyi cengci*} to the strategic level {*zhanlue cengci*}. This also illustrated that IO under informationized conditions {*xinxihua tiaojianxia*} had already been interwoven together with other operational activities, to become the main factor {*yinsu*} influencing enemy decision-making capability.

[24] Translator's note: translation taken directly from JP 3-13; pinyin is added to clarify variant usage.

2. Integrated {*zonghe yiti*} IO capability is the foundation for realizing IO goals.

The US military holds that in order to achieve the fundamental goal of IO, viz., seizing decision-making superiority within the operational process, it is necessary to build and fully bring into play an integrated IO capability. In the 2006 version of joint *Information Operations* regulations, the US military laid out an even clearer and all-around demarcation of IO capability, viz., IO capability includes core capabilities, supporting capabilities, and related capabilities. IO supporting capabilities directly or indirectly influence the information environment, and together with core capabilities form an organic whole {*yiti*}. Only by their adjusted-coordinated application {*xietiao yunyong*} can even better IO effects be obtained. The employment rules {*shiyong guize*} for the IO associated capabilities are not subject to the restrictions of IO; as long as these aspects are given consideration when planning {*jihua*} and conducting IO, they enable in an even better way achieving the goals of integrated-whole operations {*zhengti zuozhan*}.

3. Information reconnaissance {*xinxi zhencha*} with equal emphasis on peacetime and wartime {*pingzhan bingzhong*} is a prerequisite for conducing IO.

Within the operational process, in order to seize information superiority and then seize decision-making superiority, the US military attaches the highest importance to conducting information reconnaissance with a mutual combination of peacetime and wartime [reconnaissance]. The US military holds that combined peacetime-wartime information reconnaissance not only is an important component {*zucheng bufen*} in seizing information superiority and then seizing decision-making superiority, but at the same time also is the basis and prerequisite for organizing and conducting other IO activities. In peacetime, the US military always employs many and varied reconnaissance means {*zhencha shouduan*}, including reconnaissance satellites {*zhencha weixing*}, reconnaissance aircraft, reconnaissance ships {*zhencha chuan*}, and ground reconnaissance stations {*dimian zhencha zhan*}, to conduct uninterrupted {*bujianduan*} information reconnaissance against several susceptible areas {*mingan diqu*}, so as to acquire large amounts of important information intelligence {*xinxi qingbao*}. **[end of page 391]** In wartime, the US military, with peacetime information reconnaissance as the foundation, concentrates strengths {*jizhong liliang*} to conduct all-around and careful reconnaissance against the enemy's military information systems.

4. Integrated soft and hard kill {*ruanying shashang yiti*} information attack {*xinxi gongji*} is the main means of IO.

Since the US military has grasped the most advanced IT and has the most advanced information attack weapons, in order to achieve the goals of its IO it thus always stresses bringing into play the superiority of information attack capability, to conduct information attacks on the enemy in which integrated means {*zonghe shouduan*} are simultaneously used and soft and hard kill are integrated. Via such powerful information attacks, it stresses creating enemy C2 imbalances {*shitiao*}, communication interrupts {*tongxin zhongduan*}, and intelligence and reconnaissance system dysfunction

{*qingbao zhencha xitong shiling*}, so as to gain information superiority and then gain decision-making superiority. In the 1991 Gulf War, the US military conducted a series of electronic attack {*dianzi gongji*} activities against Iraq, which caused the air defense system {*fangkong xitong*} painstakingly built up {苦心经营 *kuxin jingying*} by the Iraqis for over a decade to lack scope for its abilities {无用武之地 *wuyong wu zhidi*}.

5. Full-dimensional seamless information protection {*quanwei wufeng de xinxi fanghu*} is assurance for the smooth implementation of IO.

The US military emphasizes that while executing powerful information attacks, it must at the same time implement full-dimensional seamless information protection. The US military clearly points out that the vulnerability {*yisunxing*} and fragility {*cuiruoxing*} of the information infrastructure {*xinxi jichu sheshi*} cause information systems to sink into paralysis {*tanhuan*} or information to leak out {*xinxi waixie*}, thus leading to losses which are ever more prominent, and even possibly leading to the failure of military activities. Following on the improvements in the operational opponent's level of mastery and application of IT, it must adopt multiple measures to implement full-dimensional, seamless information protection. In regard to the security protection {*anquan fanghu*} problem for military information systems, the US military is even worried that "electronic Pearl Harbor" incidents may ultimately occur. In order to boost information protection capability {*xinxi fanghu nengli*}, the US military emphasizes the adoption of IO simulation exercises {*moni yanxi*}, to look for and discover the weak points of one's own information infrastructure, and in view of those weak points to put forth the corresponding countermeasures {*duice*} and recommendations. At the same time, it requires that all services {*junzhong*} and all Department of Defense [DoD] associated directly subordinate institutions {*xiangguan zhishu jigou*} establish rapid reaction elements, such as computer contingency detachments {*jisuanji yingji fendui*} and automatic system security contingency detachments {*zidonghua xitong anquan yingji fendui*}, so that information systems after being damaged can obtain timely repair. **[end of page 392]**

(2) Basic principles

The US military holds that IO should purposefully {有目的地 *you mudidi*} make the "fog of war" {*zhanzheng "miwu"*} facing the operational opponent become even thicker, and at the same time to bring into play friendly high-tech superiority, so as to dispel the "fog of war" facing the friendly side, and ensure that the adversary's inferiority cannot be changed into a superiority. Hence, the US military holds that IO is a newly developing operational pattern, having distinct characteristics {*tedian*}, and that when organizing and implementing IO, [its forces] generally must abide by the following principles.

1. Principle of decapitation {*zhanshou*}

The principle of decapitation signifies conducting information attacks on the decision-making institutions of units at all levels in the enemy, i.e., the enemy's national command authority [NCA] {*guojia zhihui dangju*}, Joint Staff {*lianhe canmoubu*}, and theater general headquarters [HQ] {*zhanqu zong silingbu*}, as well as the HQs {*silingbu*} of all field group armies, divisions, and battalions {*yezhan jituanjun, shi, he ying*}, to prevent the enemy's C2 personnel from using automated or electronic assisted decision-making means {*fuzhu juece shouduan*}. It emphasizes attacking the enemy's head {*toubu*}, not its body {*quti*}, and not allowing the enemy to prevent the friendly side from purposefully creating the "fog of war;" severing or disrupting all of the enemy's information broadcast media {*xinxi chuanmei*} telephone, radio spectrum {*wuxiandian pinpu*}, fiberoptic cable {*dianlan*}, and other transmission means; severing the enemy's nervous system {*shenjing xitong*}, and paralyzing, disrupting, weakening, or destroying the enemy's various transmission devices {*chuanshu zhuangzhi*}; stopping the enemy from using grey systems {*"huise" xitong*}, so that the enemy cannot employ 3rd-party communication satellites; and thinking up ways to create disorder {*hunluan*} and terror {*kongbu*}, to ensure that after the enemy's head is knocked off, its body cannot be active.

2. Principle of blinding {*zhimang*}

The principle of blinding signifies first destroying the enemy's detection instrument equipment {*tance qicai*} such as sensors {*chuanganqi*}, rather than wiping out {*xiaomie*} enemy personnel. The US military holds that under informationized conditions, the original offensive and defensive theory {*jingong yu fangyu lilun*} is no longer applicable, and that commanders {*zhihuiguan*} should think up ways to first destroy the enemy's sensors, so that the enemy becomes deaf and blind. It stresses combining the use of auto-homing weapons {自动寻的武器 *zidong xundi wuqi*} and electronic jamming {*dianzi ganrao*} with soft and hard suppression means {*ruanying yazhi shouduan*} against the enemy's air defense firepower {*fangkong huoli*}, to prevent the enemy's electronic equipment {*dianzi zhuangbei*} from transmitting electromagnetic [EM] signals. Against broad-spectrum video observation instruments {*kuanpinpu shixiang guanceyi*} which the enemy can employ, [commanders] must use focused-energy {*jujiaoneng*}, band-energy {*pindaineng*}, ultrahigh-energy {*chaoqiangneng*}, or intelligent conventional weapons {*zhinengxing changgui wuqi*} to deal with them. **[end of page 393]** At the same time, it emphasizes suppressing the enemy's passive sensors {*beidong chuanganqi*}, and will use lasers {*jiguangqi*} to irradiate the enemy's optical tracking instruments {*guangxue genzongyi*}, fry {*zhahui*} the enemy's radio-frequency [RF] receivers {*shepin jieshouji*}, and burn up {*shaohui*} the enemy's passive detectors {*beidong tanceqi*}. In sum, commanders should think up ways to "blind" all of the enemy's sensors, so that the enemy "cannot see clearly" {*"kanbuqing"*} everything which is about to occur. The US military stresses that any sensors which provide information to the enemy all must be viewed as the enemy's sensors. [Commanders] should force the grey systems to closely cooperate with the friendly side, and not permit

3rd-party satellites which execute meteorological data collection, earth detection {*diqiu tance*}, and other missions to provide information to the enemy.

3. Principle of battlefield transparency {*zhancheng touming*}

Commanders should be crystal clear {一清二楚 *yiqing erchu*} about the battlefield situation in every kind of respect, and accomplish from start to finish making the battlefield transparent. To this end, commanders should think of ways to ensure that friendly surveillance {*jianshi*} and reconnaissance are uninterrupted, rigorous {*yanmi*}, and multispectral {*duopinpu*}. They must not ignore the offensive routes of which the enemy is "not very capable" {*"butai keneng"*}, and must penetrate clouds, rainfall, dark of night, and the penetrable earth's surface {*kechuantou dibiao*} to carry out observation; they must not fear consuming energy and sensor instrument equipment {*chuangan qicai*}; they must see that friendly activities always are conducted before the enemy is in the cyclical process of "awareness–feedback" {*"renshi–fankui"*}, and must exploit all opportunities to always be one step ahead of the enemy. They [must] ensure completely receiving the sensor data sent by joint forces {*lianhe budui*} from long distances, and avoid transporting {*shusong*} too much sensor information over vulnerable communication nodes {*cuiruode tongxin jiedian*}; they must not spend too much time in processing data, unless they have no other choice but to do so; and they must directly distribute {*fenfa*} the data to all shooters {*sheshou*}, so that they can immediately use it. [Commanders must] ensure carrying out battle damage assessment [BDA] {*zhandou huishang pinggu*} in a rapid, all-around, and accurate manner. They must not waste resources on false targets {*jiamubiao*} or on already damaged targets {*cuihui de mubiao*}. They must exploit [cases of] multiple phenomenology {多重现象学 *duochong xianxiangxue*}, and from among the fixed targets accurately recognize the targets having activity {*huodong de mubiao*}.

4. Principle of agility {*minjie*}

The principle of agility requires that commanders should ensure that the friendly decision-making cycle is shorter than the enemy's decision-making cycle, and moreover that [friendly] operations {*yunxing*} are faster. When executing the principle of decapitation, the principle of blinding, and the principle of battlefield transparency, they must see that [those principles] are mutually in concert [complemented] {*xianghu peihe*}.They must see that the friendly side's **[end of page 394]** single process of "shoot–move–reshoot" {*"sheji–yundong–zaisheji"*} is carried out faster and more accurately, while the enemy always remains in a state {*zhuangtai*} of "taking a beating–shock–taking another beating" {*"aida–zhenjing–zai aida"*}, and that the enemy from start to finish does not know the friendly activities direction {*xingdong fangxiang*}. Hence, [this principle] requires that the information providers should maintain a high state of readiness {*zhanbei zhuangtai*}; ensure at all times providing all information needed and required {*xuyao*}; and ensure that all-around, complete, and already checked intelligence {*hedui de qingbao*} and target information are provided before needed by the shooters. It changes the usually encountered situation in which the attack aircraft pilots {*gongjiji*

jiashiyuan} when preparing for takeoff have no choice but to wait for the latest intelligence. At the same time, it requires that the frequency bandwidth {*pindai kuandu*} must ensure full throughput {*quanliang tongguo*} of the data, and leave a certain leeway. It precludes the use of easily jammed and vulnerable communication means to send important information; and it precludes using narrow-band {*pindaizhai*}, slow-speed communication media to send large quantities of information, to avoid communication "bottleneck"-induced congestion of the lines over which the decision-makers acquire information.

5. Principle of survival {*shengcun*}

The principle of survival emphasizes that commanders should employ multiple avenues to avoid being easily decapitated by the enemy. To this end, it stresses centralized formulation of tactics and planning {*jizhong zhiding celue yu jihua*}, but decentralized {*fensan*} implementation of plans for use of military forces {*yongbing jihua*}; bringing into play the initiative [quality] {*zhudongxing*} and flexibility {*linghuoxing*} of their subordinate troops, to avoid implementing overly centralized C2; exploiting all resources of the nation, and using all means of the entire society and all departments (TV news broadcasts, computer or communication systems, communication satellites, fax machines, electronic billboards, and international general-purpose networks {*guoji tongyong wangluo*}) to ensure smoothness of information flow; adopting multi-node, multi-system, multipath, multi-frequency transmission of information {*chuandi xinxi*}, to boost survivability {*shengcun nengli*}; concealing {*yinbi*} friendly command, control, and communication [C3] systems, using mobile small satellite receiving devices {*kejidong de xiaoxing weixing jieshou zhuangzhi*}, and frequently changing their deployment location {*peizhi weizhi*}; burying of electric cable and fiberoptic lines {*guangxian xianlu*} between fixed firing positions {*fashe zhendi*}; transmitting deception signals {*qipian xinhao*} from secondary nodes; and from start to finish, retaining backup communication plans {*beiyong tongxin jihua*}, and [seeing that] the backup communication plans should have stronger survivability than the main communication plan. When ascertaining if the enemy has the facilities equipment {*shebei*} and capability for jamming the r.f. [band], [commanders] should not use r.f. transceivers {*diantai*} to replace the basic telephone communication system. To ensure that the friendly side **[end of page 395]** possesses technical superiority in C3 respects, they should make sure to be ahead of the enemy in respect to renewing IT [based] equipment {*zhuangbei*}. To this end, they must invest more funds {*zijin*}; but they cannot, in order to buy more weapons and ammunition {*wuqi danyao*}, reduce the research and development [R&D] {*yanzhi*} outlays in C3 technology and equipment respects.

6. Principle of compatibility {*jianrong*}

The principle of compatibility emphasizes that all types of information systems not only must avoid system vulnerability {*cuiruoxing*} brought about by standardized design {*biaozhunhua sheji*}, but also must overcome the joint operations requirements {*lianhe zuozhan yaoqiu*} independently developed by all services in the past, which could

not achieve interconnection and intercommunication {*hulian hutong*}, which could not realize sharing {*gongxiang*} of resources and information, which lacked unified security and secrecy {*tongyide anquan baomi*} measures, which had low integrated-whole operational effectiveness {*zhengti zuozhan xiaoneng*}, and which could not be adapted to fairly low ranks {*jibie*}. Within informationized war, [commanders] should pursue diversification and mutually compatible {*xianghu jianrong*} C3 systems, and further perfect global control systems {*quanqiu kongzhi xitong*} which are interoperable {*kecaozuo*}, have resources sharing, are highly mobile {*jidong*}, are seamlessly interconnected {*wufengxi lianjie*}, and have high survivability.

7. Principle of differential {级差 *jicha*}

The principle of differential emphasizes not fighting a low-rank war {*dijibie de zhanzheng*} with a low-rank enemy. It holds that if Information Age armed forces are faced with Agricultural Age or Industrial Age armed forces, they should not fight an Agricultural Age or Industrial Age war, but rather an Information Age war. Since the battlefield environment under informationized conditions shows a good many inherent weak points, the adversary will fully exploit these weak points to conduct operations against the friendly side. Since the engaging sides {*jiaozhan shuangfang*} when confronted with the "fog of war" both will be extremely vulnerable, both will need to carry out signal communication {*tongxin lianluo*}. However, under the usual circumstances, IT can ensure that the friendly side will not encounter the adversary's surprise raids {*turan xiji*}; it enables the adversary's maneuver {*jidong*} and reinforcement activity {*zengyuan huodong*} to be always within friendly surveillance and grasp, and may subject the adversary to friendly attacks. Hence, commanders should seek to have the "fog of war" confronting the operational opponent become denser and disrupt the enemy's methods of communication, and employ better intelligence means and weapons with better strike precision {*daji jingdu*} and higher effectiveness and lethality {*shashangli*} to cleverly conduct operations. **[end of page 396]**

II. IO strengths of the US military…397

The IO strengths are the material basis for carrying out IO missions. In recent years, the US military, according to the needs {*xiqiu*} of IO theory, has given impetus to IO strength building {*liliang jianshe*}, and in the units of all services has energetically developed IO units and equipment. The US military's IO strengths mainly are composed of EW, PSYOP, and CNO strengths.

(1) Electronic warfare strengths

1. Navy EW strengths

The US Navy EW force-strengths {*bingli*} are completely woven into the Navy's operational units {*haijun zuozhan budui*}, and are under the command of the Chief of Naval Operations {*haijun zuozhan buzhang*}. Altogether they are organized into 16 EW

aircraft squadrons {*zhongdui*}, and each squadron is organized to have 4 EA-6B EW aircraft.

The Pacific Fleet aviation forces {*taipingyang jiandui hangkongbing*} are organized into 9 EA-6B EW aircraft squadrons, the Atlantic Fleet {*daxiyang jiandui*} aviation forces are organized into 6 EA-6B EW squadrons, and the Naval Reserves {*haijun yubeidui*} aviation forces have 1 EA-6B EW squadron.

Medium-sized and larger operational ships {*zhongxing yishang de zuozhan jianzhi*}, such as aircraft carriers {*hangkong mujian*}, battleships {*zhanliejian*}, cruisers {*xunyangjian*}, destroyers {*quzhujian*}, frigates [escort vessels] {*huweijian*}, amphibious ships {*liangqijian*}, and auxiliaries {*fuzhujian*}, as well as the operations departments of submarines {*qianting de zuozhan bumen*}, all are organized to have the corresponding EW sub-units {*qudui*}.

2. Air Force EW strengths

The US Air Force [USAF] EW units adopt the air group {*dadui*} or squadron organizational structure {*bianzhi*}, and are mainly equipped with special-purpose electronic jamming aircraft and anti-radiation missile [ARM] {*fanfushe daodan*} attack aircraft {*gongji feiji*}.

USAF altogether organizes 6 squadrons of special-purpose electronic jamming aircraft, each squadron organized with 5 EC-130H ["Compass Call"] EW aircraft, except for 2 of these squadrons, which each are organized with 7 EC-130H EW aircraft. The other 4 combat aircraft {*zhandouji*} squadrons are organized to have up to 10 FC-16CJ (capable of executing EW missions) ["Fighting Falcon"] aircraft.

3. Marine Corps {*haijun luzhandui*} EW strengths

The US Marine Corp [USMC] aviation forces' EW units are organized into 4 squadrons of EA-6B EW **[end of page 397]** aircraft, each squadron organized with 5 EA-6B EW aircraft. The ground EW units are organized into 2 ground EW battalions {*dimian dianzizhan ying*}, respectively attached {*peishu*} to the Pacific and Atlantic Fleet Marine Commands {*luzhandui silingbu*}.

4. Army {*lujun*} EW strengths

The US Army's active-duty {*xianyi*} operational units altogether are organized to have 11 intelligence brigades {*qingbao lu*}, 18 military intelligence battalions {*junshi qingbao ying*}, and 17 military intelligence companies {*junshi qingbao lian*}. In addition, the Army Intelligence and Security Command [INSCOM] {*lujun qingbao yu baomi silingbu*} also organizes 6 military intelligence groups {*junshi qingbao dadui*}.

(i) Corps-subordinate EW units {*junshu dianzizhan budui*}

The US Army's various corps each are organized with 1 military intelligence brigade, mainly organized into a HQ {*silingbu*}, associated directly subordinate detachments, operations battalion {*zuozhan ying*}, tactical exploitation battalion {*zhanshu liyong ying*}, and air exploitation battalion {*kongzhong liyong ying*}. Their main mission is to exploit the strengths and means within the task organization {*biancheng*} to provide the corps and all of its subordinate divisions with operational intelligence, imagery intelligence [IMINT] {*tuxiang qingbao*}, and signals intelligence [SIGINT] {*xinhao qingbao*} support , as well as with EW support and counterintelligence {*fanqingbao*} support. Of these, the main mission of the HQ and its directly subordinate detachments is to provide the planning, management, and adjusting-coordination needed for employing the intelligence brigade force-strengths. The main missions of the military intelligence brigade's operations center include the following: under the guidance {*zhidao*} of the military intelligence brigade commander, to be responsible for planning and management and for implementing technical control of and mission distribution {*renwu fenpei*} for the brigade's force strengths; to process intercepted {*zhenshou*} SIGINT and EW data, and arrange and publish {*zhengli, bianyin*} the SIGINT; to carry out contact with and exchange data with the technical control and analysis teams {*jishu kongzhi he fenxi zu*} of the divisions, armored cavalry regiments {*zhuangjia qibing tuan*}, and independent brigades; and to maintain contact with corps-level and higher command institutions {*zhihui jigou*} and national associated systems {*guojia xiangguan xitong*}, so as to realize fusion of the technical data {*jishu shuju ronghe*} generated by tactical units with technical data of the national-level associated systems. The main missions of the operations battalion are as follows: to be responsible for providing support detachments {*fendui*} used for reinforcing {*jiaqiang*} the tactical operations centers of the corps intelligence officer and operations officer, and for providing 1 technical control and analysis team, used for supporting the intelligence brigade operations officer's unit management and to the corps intelligence officer's SIGINT data analysis; and to provide communication support to the intelligence brigade. The tactical exploitation battalion is the element {*fendui*} which mainly executes electronic offense {*dianzi jingong*} missions. Its main missions are as follows: to provide the corps and its main subordinate detachments with ground **[end of page 398]** EW, interrogation of prisoners of war [POWs] {*shenfu*}, and counterintelligence support; and when obtaining corps higher-level echelon reinforcement {*jun shangji tidui jiaqiang*}, it also must provide technical intelligence, particularly collection and technical support. The air exploitation battalion's main missions are as follows: to provide the corps with air surveillance {*kongzhong jianshi*} and air SIGINT support, and to provide communication intelligence [COMINT] {*tongxin qingbao*} and electronic intelligence [ELINT] {*dianzi qingbao*} support. The corps-subordinate intelligence brigade is mainly used for dealing with enemy 1st-echelon division(s) within the corps operations zone {*zuozhan diyu*}, while the mission of dealing with the enemy's 2nd echelon then is given support by USAF systems and national systems.

(ii) Division-subordinate EW units {*shishu dianzizhan budui*}

US Army infantry divisions {*bubing shi*}, armored divisions {*zhuangjia shi*}, mechanized divisions {*jiexiehua shi*}, air assault divisions {*kongzhong tuji shi*}, and air landing divisions {*kongjiang shi*} all are organized with military intelligence battalions, and mainly are organized with battalion HQs {*yingbu*} and with operations companies {*zuozhan lian*}, intelligence and surveillance companies {*qingbao yu jianshi lian*}, and service support companies {*qinwu zhiyuan lian*}. Their main mission is to provide the division commander with intelligence, EW, and counterintelligence support, and at the same time to support all operational activities of the division. In this, the main mission of the battalion HQ and operations company is to be responsible for the adjusting-coordination, organization, and implementation of intelligence and EW work; the battalion commander usually controls and guides all military intelligence resources within the organizational system {*jianzhi*}, as well as those of the attached supply divisions {配属给师 *peishu jishi*} and support divisions. The battalion operations center mainly is responsible for putting into effect unified management of the organizational-system resources and support resources of the battalion, to meet the intelligence and EW requirements of the division intelligence officer and operations officer; the EW company is the element which mainly executes electronic offense missions, its main mission being to provide the division with EW support and SIGINT support. The main missions of the EW platoon {*pai*} are to be responsible for intelligence collection and analysis, as well as organizing and implementing electronic jamming, and to provide the brigade with battlefield surveillance and OPSEC support. One EW platoon usually supports 1 brigade or the operational activities within the brigade operations zone; a SIGINT processing platoon can perform certain processing of intercepted signals {*jiehuo xinhao*}; and the intelligence and surveillance company is responsible for providing the division with ground radar surveillance {*dimian leida jianshi*}, counterintelligence, and POW-interrogation support. The service support company is responsible for providing the battalion with provisions, service, and mechanical and communication electronic maintenance {*weihu*}, as well as communication support. The division, besides the resources within the organizational system, usually also can obtain the support of the corps-subordinate EW companies' operations platoons. The division-subordinate military intelligence battalions mainly are used for dealing with an enemy division's 1st echelon. **[end of page 399]**

(iii) Regiment (brigade)-subordinate EW units {*tuan (lu) shu dianzizhan budui*}

The US Army's armored cavalry regiments or independent brigades all are organized with military intelligence companies, each company having under its command a communication platoon, operational support platoon, surveillance platoon, collection and jamming platoon {*souji yu ganrao pai*}, and technical control and analysis detachment, as well as a flight platoon {*feixing pai*}. Of these, the main mission of the communication platoon is to provide personnel and facilities equipment for managing or employing the company's telecom business affairs {*dianxin shangwu*} and radio-teletypes [RTTY] {*wuxiandian dianchuan daziji*}. The main mission of the surveillance

platoon is to provide a ground surveillance radar team {*dimian jianshi leida zu*} for battlefield surveillance and early warning, to adapt to missions assigned {*fenpei*} by the regimental tactical center's support detachment. The collection and jamming platoon is the element which mainly executes electronic offense missions, its main mission being to carry out collection of voice communication {*yuyin tongxin*}, so as to carry out high-frequency [HF] or very-high-frequency [VHF] communication jamming {*gaopin huo shengaopin tongxin ganrao*}. The technical control and analysis detachment is set up in a military intelligence company's tactical operations center; its main missions are to receive electronic jamming missions assigned by an armored cavalry regiment's operations officer or firepower support detachment, and SIGINT and electronic reconnaissance {*dianzi zhencha*} missions assigned by the intelligence officer, and to specifically assign these missions within the military intelligence company, as well as carry out technical control. The flight platoon is set up in the combat aviation squadron {*zhandou hangkong zhongdui*}; its main missions are to receive operational control by the technical control and analysis detachment, and to supplement {*buchong*} the ground EW resources by providing airborne communication intercept {*jizai tongxin jieshou*}, direction finding {*cexiang*}, and jamming support.

(2) Network warfare [CNO] strengths {*wangluozhan liliang*}

Beginning in the 1980s, the US military set about establishing CNO units {*jisuanji wangluozhan budui*}, whose main missions are key point guarding against {*zhongdian fangfan*} computer information leaks {*xielou*}, soft- and hard-kill {*ruanying shashang*} attacks suffered by computers, and computer virus {*jisuanji bingdu*} and computer hacker {*heike*} attacks.

1. Navy network warfare strengths

US Navy units associated with conducting CNO mainly include the following: the Office of the Chief of Naval Operations [OpNav] {*haijun zuozhan bu*} Naval Network Operations Command [NNOC or NAVNETOPSCOM] {*haijun wangluo zuozhan silingbu*}, and its subordinate Navy/Marine Corps Intranet Task Force {*neilianwang teqiandui*}, the Navy Computer and Telecommunications Command [NAVCOMTELCOM] {*haijun jisuanji yu dianxin silingbu*}, and the Navy Computer Network Defense [CND] Task Force {*haijun jisuanji wangluo fangyu teqiandui*}. Their main missions are to carry out surveillance, reconnaissance, analysis, and reporting of "intrusion incidents" {*"ruqin shijian"*} of unauthorized intrusion into {*weishouquan chuangru*} US Navy networks, and to adopt responsive measures. **[end of page 400]**

2. Air Force network warfare strengths

USAF units associated with conducting CNO mainly include the following: Pacific Air Forces' [PACAF] {*taipingyang kongjun siingbu*} Seventh Air Force {*di 7 hangkong bu*}, 607th Air Intelligence Group {*kongzhong qingbao dadui*}, 607th IW Flight {*xinxizhan xiaodui*}; Air Combat Command's [ACC] {*kongzhong zuozhan silingbu*} Air

Intelligence Agency {*kongjun qingbao ju*}, 90th IO squadron and 318th IO Group (under which are the 23rd IO Squadron, 39th IO Squadron, and 92nd IO Intruders Squadron {*xinxi zuozhan ruqinzhe zhongdui*}); Air Intelligence Center's 53rd Computer System Squadron; Eighth Air Force's 67th IO Wing {*liandui*} (under which are the 26th, 692nd, 67th, and 544th IO Groups) and 690th IO Group (under which is the 690th Computer Support Squadron); and the Ninth Air Force's 609th IO Squadron, which is the computer contingency response detachment {*jisuanji yingji fanying fendui*} with the highest professional standards {*zhuanye shuiping*} among all services. This detachment, mainly via downloading {*xiazai*} situations of accessing {*fangwen*} computer networks over the previous 24 hours, grasps activity of unlawful intrusion {*feifa ruqiin*} into information networks, in real time detects activity of unlawful intrusion into information networks, and adopts information defense measures having a directed [focused] quality {*zhenduixing*}.

3. Army network warfare strengths

The US Army, in order to organize and conduct CNO, specially established the 1st IO Command {*xinxi zuozhan silingbu*} within INSCOM. This command is responsible for adjusting-coordinating and guiding the defense of Army computer systems and networks, as well as adjusting-coordinating and conducting computer attacks {*jisuanji gongji*} in order to realize the intent {*yitu*} of the operational command commanders {*zuozhan silingbu siling*}. The Office of the Chief, Army Reserve [OCAR] {*mei lujun houbeiyiju juzhang bangongshi*} also established the Army Reserve IW Command {*xinxizhan silingbu*}, composed of a certain number of computer contingency response units {*xiaodui*}, information infrastructure defensive support units {*fangyu yuanzhu xiaodui*}, technical research units, and subordinate networks; its main mission is to conduct CND and information support {*baozhang*}. Of these, the main missions of the computer contingency response units are to carry out identification {*shibie*}, response, analysis, and reporting of or to computer intrusion incidents, and to implement continuous surveillance of the Defense Research and Engineering Network [DREN] {*guofang yanjiu yu gongcheng wang*}; the main mission of the information infrastructure defensive support units is to provide weak point evaluation assessment {*ruodian pinggu*} and network and computer ruggedizing services {*jiagu fuwu*}, and to provide support {*zhichi*} to the DoD Information Technology **[end of page 401]** Security Certification and Accreditation Process [DITSCAP] {*anquan renzheng yu jianding jihua*}; and the main missions of the technical research units are to be responsible for verifying security technology {*yanzheng baomi jishu*}, skills, and programs {*chengxu*}, and to carry out security testing {*baomi shiyan*} and evaluation.

(3) PSYOP strengths

To strengthen command of PSYOP, the US military has established specialized PSYOP command institutions. Strategic-level PSYOP command institutions mainly include the International Communication Agency [ICA] {*guoji jiaoliu shu*} and the Joint Public Affairs Department of the National Security Council [NSC]. Campaign-level

PSYOP command institutions mainly include the temporary-quality {*linshixing*} PSYOP command institutions composed of related personnel from the theater commands {*zhanqu silingbu*}, Special Operations Command [SOCOM] {*tezhong zuozhan silingbu*}, and PSYOP units {*budui*}. The tactical level, then, is specifically organized and conducted mainly by the various PSYOP support companies.

1. Navy PSYOP strengths

The Office of the Chief of Naval Operations [OpNav] is the execution department and supreme decision-making institution for commanding naval PSYOP activities. Naval Special War Group 1 and Group 2 {*di1, di2 tezhong zuozhan dadui*} under the Naval Special Warfare Command [NAVSPECWARCOM, NAVSOC, or NSWC] {*haijun tezhong zuozhan silingbu*} undertake PSYOP missions, and are responsible for the application of PSYOP within naval special operations.

2. Air Force PSYOP strengths

Air Force Special Operations Command [AFSOC] {*kongjun tezhong zuozhan silingbu*} is responsible for the organization and application of PSYOP within Air Force special operations. The Air Force IW Center set up under the Air Intelligence Agency {*kongzhong qingbao ju*} [now the Air Force ISR Agency] is responsible for the formulation of PSYOP plans, and provides PSYOP training {*xunlian*} for the related personnel. All major commands [MAJCOMs] {*da silingbu*} of the Air Force are responsible for the associated training and for adjusting-coordinating the associated intelligence, feedback, logistics {*houqin*}, and communication support. The 193rd Special Operations Squadron under the command of the 193rd Special Operations Wing subordinate to AFSOC is equipped with EC-130E PSYOP aircraft {*xinlizhan feiji*}. Besides undertaking regular support missions, it also provides PSYOP units {*budui*} with radio/wireless communication interrupt {无线电通讯中断 *wuxiandian tongxun zhongduan*} and TV rebroadcast {*dianshi zhuanbo*} missions.

3. Army PSYOP strengths

The US Army Staff {*lujun canmoubu*} is the executing department and high-level advisory [body] {*gaoji guwen*} for commanding Army PSYOP, and is the supreme decision-making institution for PSYOP activities. Army Special Operations Command [USASOC] {*lujun tezhong zuozhan silingbu*} **[end of page 402]** is responsible for the application of PSYOP within Army special operations. Within the commands subordinate to USASOC there is 1 Army Directorate of Civil Affairs and Psychological Operations {*lujun minshi yu xinxlizhan silingbu*}. The main missions of this directorate are to be responsible for formulating wartime PSYOP plans, to participate in peacetime PSYOP exercises, to guide the training of [Army] Reserve PSYOP units, and to be responsible for providing PSYOP consultations {*zixun*} to the next-higher-level commands.

At present, the US military's PSYOP units include 1 active-duty PSYOP group {*dadui*} (also called the 4th PSYOP Group) and 2 Army Reserve PSYOP groups. Under the command of the 4th PSYOP Group are 6 PSYOP battalions; these are the core for all of the US military's PSYOP units, and are equipped with printing and copying equipment, fixed and mobile transceivers, TV and film instruments {*qixie*}, radio intercept {*wuxiandian zhenting*} [equipment], and communication facilities equipment which can automatically carry out information processing. The PSYOP battalions subordinate to the PSYOP groups are divided into four types {*lei*}: general support battalions, direct support battalions, POW work {*zhanfu gongzuo*} support battalions, and mass work {*minzhong gongzuo*} support battalions. The PSYOP companies are the units {*danwei*} subordinate to the battalions, and mainly include the following: printing companies, [radio] broadcasting companies {*guangbo lian*}, communication companies, area support companies, propaganda companies, and PSYOP research and analysis companies. The 2nd and 7th Army Reserve PSYOP Groups each have command over 4 PSYOP battalions. They are mainly responsible for conducting reconnaissance within the theater scope, for providing technology and instrument equipment {*jishu qicai*} for the organizational-structure propaganda materials {*bianzhi xuanchuan cailiao*} of other PSYOP units within the root theater, and for performing work with POWs and occupied-area inhabitants {*zhanlingqu jumin*}; within corps and division HQs {*silingbu*}, they draft {*nizhi*} plans for conducting tactical PSYOP, and ensure the realization of the campaign resolution {*zhanyi juexin*}.

III. Main activities of the US military's IO…403

The US military divides IO into two large types: offensive [quality] IO activities {*jingongxing xinxi zuozhan xingdong*} and defensive [quality] IO activities {*fangyuxing xinxi zuozhan xingdong*}.

(1) Offensive IO activities

Offensive IO activities include EW, CNO, PSYOP, OPSEC, and MILDEC. Some of these activities belong to the indirect-quality {*jianjiexing*} ones, such as PSYOP, OPSEC, and MILDEC, while EW and CNO **[end of page 403]** belong to direct-quality offensive activities. The US military holds that in the specific implementation process, the above activities must be integrated in application {*zonghe yunyong*}.

1. Electronic warfare

The US military holds that EW is an important form {形式 *xingshi*} of IO, and within IO the US military emphasizes regarding EW mandatorily used in the first battle {*shouzhan biyong*} and penetrating from start to finish as an important means for winning wars. Via integrated application of a variety of offensive and defensive tactics and techniques, one influences, corrupts {*raoluan*}, and [/or] exploits the enemy's use of the EM spectrum, and at the same time protects the friendly use of the EM spectrum. EW signifies military activities which employ EM energy and [/or] directed energy

{*dingxiang neng*} to control the EM spectrum or to attack the enemy. Usually it is divided into three types: electronic attack, electronic protection {*dianzi fanghu*}, and EW support.

Electronic attack is the basic means of offensive-quality IO. Mainly via means such as use of electronic jamming, electronic deception {*dianzi qipian*}, and directed-energy or anti-radiation weapons {*dingxiang neng huo fanfushe wuqi*}, one attacks the enemy's personnel and installations {*sheshi*} or equipment, prevents the enemy's effective use of the EM spectrum, and [thus] achieves the goals of destroying, weakening, or disrupting {*pohuai*} the enemy's combat power {*zhandouli*}. Electronic attack usually is employed in combination with other attacking {*gongjixing*} means, such as integrated implementation of electronic attack and lethal-quality firepower {*shashangxing huoli*}, and thus can become a "multiplier" {*"beizengqi"*} of combat power.

Electronic protection signifies the self-protective {*ziwo baohuxing*} electronic jamming and electronic radiation control activities adopted in order to protect the friendly use of the EM spectrum.

EW support [or electronic support measures (ESM)] signifies carrying out detection, identification, and positioning {*tance, shibie he dingwei*} of the enemy's intentional or unintentional EM-energy radiation sources {*fusheyuan*}; assisting commanders at all levels in grasping and understanding the battlefield posture {*zhanchang taishi*}; and assessing {*panduan*} the threat coming from the enemy. EW support mainly indicates services {*fuwu*} to conduct electronic attack and electronic protection plus other tactical activities, such as providing the needed information for decision-making on target positioning {*mubiao dingwei*}, target vectoring {*mubiao yindao*}, and threat warning {*weixie baojing*}. It is the embodiment of the timely reaction capability between combat information and the sensor-shooter system {*chuanganqi–sheshou xitong*}. EW support generally is conducted during peacetime periods, but also can be carried out in crisis or conflict periods. **[end of page 404]**

2. Computer network operations

Computer network attack [CNA] {*jisuanji wangluo gongji*} indicates the various activities to carry out corruption, blocking {*zu'ai*}, weakening, or disruption of the information or computers residing within computer networks, and against the computer networks themselves. The US military's current CNA mainly relies on data flow to execute the attacks, and usually is divided into three modes {*moshi*}: system of systems [SoS] sabotage/disruption mode {*tixi pohuai moshi*}, information misleading mode {信息误导模式 *xinxi wudao moshi*}, and integrated mode {*zonghe moshi*}. The SoS sabotage/disruption mode, mainly via methods such as transmission of computer viruses and logic bombs {*luoji zhadan*}, disrupts the enemy's computers and network SoS, and creates paralysis of the enemy C2 system. The information misleading mode mainly transmits false intelligence {*jiaqingbao*} to enemy computers and network systems, to alter the functions {*gongneng*} of the enemy information systems, and carry out

information misleading and flow-path misleading {*liucheng wudao*} of enemy decision-making and C2. The integrated mode, then, via integrated application of the SoS sabotage/disruption mode and the information misleading mode, obtains the optimal attack effects, and [thus] achieves the goal of CNA.

3. PSYOP

The US military holds that PSYOP indicates, via transmission of pre-selected information and evidence {*zhengzhao*} to the foreign populace, influencing of their sentiment, motives, and objective inference {*keguan tuili*}, and ultimately influencing their government, organizations, groups {*tuanti*}, and individual behavior. Its goal is to lure {*yinyou*} or impel the foreign nation's attitude and activities toward development in a direction favorable to friendly objectives. The US military feels that, in terms of directly shaking the enemy's war conviction {*zhanzheng xinnian*} and destroying the enemy's spirit and will for carrying out war, PSYOP possesses powerful might {*weili*} not possessed by other operational patterns. The US military holds that soft and hard combined {*ruanying jiehe*} PSYOP already has become the highest-level operational pattern within IW, and already has risen to a strategic means which can directly shake the enemy' war will {*zhanzheng yizhi*}, and achieve the goal of troops who subdue the enemy without a battle {不战而屈人之兵 *buzhan er quren zhibing*}.

PSYOP according to its application level can be divided into strategic-level PSYOP {*zhanlueji xinlizhan*}, campaign-level PSYOP {*zhanyiji xinlizhan*}, and tactical-level PSYOP {*zhanshuji xinlizhan*}. Strategic-level PSYOP usually adopts forms such as declaring a political stance or diplomatic stance, and issuing public announcements or communiqués, to influence the enemy's decision-making layer. **[end of page 405]** Campaign-level PSYOP usually applies means such as dispersal of leaflets, loudspeaker broadcasts, radio {*diantai*} or TV broadcasts, network propaganda, and other information propagation means, to persuade the enemy to defect {*pantao*}, desert {*kaixiaocha*}, or surrender. Persistent {*chijiu*} campaign-level PSYOP offensives {*xinlizhan gongshi*} are "multipliers" of entire operational activities; they can accelerate disintegration of enemy morale {*wajie dijun shiqi*}, and in psychological terms put the enemy to rout {*jikua diren*}. Tactical-level PSYOP usually employs battlefield propaganda directed to the enemy at the front line {*zhanchang hanhua*} and other means to increase the enemy's sense of fear, break up the enemy's internal unity {*neibu de tuanjie*}, and weaken the enemy's combat power. In addition, PSYOP also can, via propaganda means such as the media, conceal the true situation {掩盖事实真相 *yangai shishi zhenxiang*} and complement the MILDEC activities.

4. OPSEC

The goal of OPSEC is to prevent the enemy from acquiring important information related to friendly military activities, so as to prolong the enemy's decision-making cycle. Battlefield intelligence brings into play an important role in victory or defeat in modern war, and intelligence which is inadequate or intelligence which is inaccurate can create

enormous losses. Hence, the US military emphasizes that one must try various devices {想方设法 *xiangfang sheaf*} to prevent the enemy commander from acquiring the necessary information, to force the enemy into having no way of acquiring accurate and timely battlefield situation, and thus achieve the goal of influencing the enemy's decision-making and military activities. OPSEC is applicable to all military activities at all levels of commands/HQs {*silingbu*}.

OPSEC is a continuous process, and penetrates the entire process from peacetime to crisis and conflict, and back to peacetime; moreover, it possesses very strong practicality {实用性 *shiyongxing*} and operability {*caozuoxing*}. OPSEC also is a set of methods applicable to any operation and military activity, and is directly used for interfering with the enemy's acquisition of important information. The missions of OPSEC include the following: to detect friendly actions {*xingwei*} which are easily observed by the enemy intelligence systems; to determine the various types of data which the enemy intelligence systems can acquire and use for deciphering {*poyi*} and grasping friendly important information; and to adopt measures to eliminate friendly weak points which can be exploited by the enemy, or to reduce them to an acceptable level.

The implementation of OPSEC usually is divided into five steps: the first is identifying important information. From the viewpoint of enemy collection of intelligence, [this involves] assessing which pieces of friendly information are of the utmost importance to the enemy. **[end of page 406]** OPSEC is not at all [just] keeping secret {*baomi*} all classified information {*yiqie shemi xinxi*}; the key point of the secrecy is "information of the utmost importance" to the enemy. Second is analyzing the threats. From among intelligence and open-source information {*gongkai de xinxi*}, one analyzes the enemy intention {*qitu*}, operational objectives {*zuozhan mubiao*}, and intelligence collection capability, plus friendly critical information {*guanjie xinxi*} which the enemy can already have grasped, and assesses the threats which can be faced by the friendly side. Third is analyzing the weak points. Combining these with the enemy's intelligence collection capability, one analyzes the friendly activities' vulnerabilities {*cuoruoxing*} and critical information whose signs {*zhenghou*} can be revealed. Fourth is evaluating the risks {*pinggu fengxian*}. Analyzing vulnerable positions {*cuiruo buwei*}, one evaluates and determines the corresponding measures for eliminating the weak points, and the effects of those measures. Fifth is adopting OPSEC activities. Usually these include three types of activities: activities control {*xingdong kongzhi*}, resistance {*duikang*}, and counter-analysis {*fanfenxi*}. The objective of activities control is to eliminate the activities signs and weak points which the enemy intelligence systems can exploit. The objectives of resistance are to disrupt the information collected by the enemy, and to render the enemy unable to identify the signs within the information. Its main measures include luring the enemy, camouflage {*weizhuang*}, concealment {*yincang*}, and interfering with or using armed force {武力 *wuli*} to eliminate the enemy's intelligence collection and processing strengths. The objective of counter-analysis is to obstruct the enemy's accurate reading {*jiedu*} of the signs, and its main measure is to conduct deception. Sixth is evaluating the effects {*xiaoguo*}, and adjusting the measures. After adopting security activities {*baomi xingdong*}, the friendly

intelligence systems still must continue to surveil the enemy's response to these measures, evaluate their effects, and further adopt activities.

5. MILDEC

MILDEC signifies activities adopted to deliberately mislead the enemy's military decision-makers {*juecezhe*} in regard to friendly military strengths, operational intention {*zuozhan qitu*}, and operational activities. It lures the enemy into adopting or halting certain activities, so as to create favorable conditions for the friendly side to fulfill its missions. Via MILDEC activities, one renders the enemy commander unable to accurately understand the friendly side's offensive capability or intention, and thus unable to most effectively apply his combat units or support units. The operational objective of MILDEC usually requires targeting {*zhixiang*} the enemy leaders having supreme decision-making authority {*zuigao juece quan*}, and the means applied usually include physical means, technical means, and management means.

Commanders at all levels all can plan {*guihua*} and conduct MILDEC, but the deception plan {*qipian jihua*} must **[end of page 407]** be formulated from the top down. The subordinate joint force commanders {*lianhe budui zhihuiguan*} should take initiative {*zhudong*} to adjust-coordinate with the higher levels; moreover, the lower levels must submit to the higher levels, to ensure the consistency of the entire deception activities plan. MILDEC is a forceful means within integrated-whole operations, but in organizing MILDEC one usually must pay a certain price. Commanders at all levels and their staff personnel must closely {*miqie*} watch the development of the state of affairs {*shitai*}, at all times weigh the advantages and disadvantages {*quanheng libi*}, and timely adjust the activities plan.

Intelligence is of the utmost importance to MILDEC, and is the basic foundation for determining the deception objectives. MILDEC activities require grasping the characteristics of the enemy's leadership layer and the process of its decision-making, and then forecasting {*yuce*} the activities which the enemy can adopt. Forecasting is the critical link {*guanjian huanjie*} in conducting MILDEC; only by accurately forecasting at what time and place the enemy will adopt what type of military activities can one accurately determine the MILDEC's operational objectives. Intelligence not only is the key to ensuring that MILDEC content is genuine and believable {*zhenshi kexin*}, but also is the foundation for evaluating the MILDEC effects and thus adopting other activities. The enemy's intelligence systems usually are not the objects {*duixiang*} of the deception, but are the channels which the deception must exploit.

(2) Defensive IO activities

The US military's defensive IO involves the integrated application of various means — information secrecy {*xinxi baomi*}, physical security {*wuli anquan*}, counter-deception {*fanqipian*}, counter-propaganda {*fanxuanchuan*}, counterintelligence, EW, and special IO {*tezhong xinxi zuozhan*} — to protect and defend {*fangwei*} the security

of friendly information and information systems. Its goals are to ensure friendly acquisition of information in a timely, accurate, and reliable manner, and to the maximum extent restrict the enemy from achieving his intention to exploit friendly information and information systems. Its main activities are composed of four mutually correlated {*xianghu guanlian*} processes: information environment protection, information attack detection {*xinxi gongji jiance*}, information capability restoration, and information attack response {*xinxi gongji fanying*}.

1. Information environment protection

The US military holds that the goals of information environment protection are to establish a protective layer for friendly information and information systems, and to prevent the enemy's intrusion into friendly systems, or reduce the threat and possibility of enemy intrusions. The content of information environment protection mainly includes hardware copying {*ruanjian kaobei*} (messages, **[end of page 408]** letters, faxes), and EM spectrum, video {*shipin*}, imagery {*tuxiang*}, audio {*yinpin*}, cable {*dianbao*}, and computer content.

During implementation of information environment protection, the joint forces commander [JFCDR] {*lianhe budui zhihuiguan*} must determine the protection scope and protection standards {*baohu biaozhun*}, conduct an analysis which synthetically integrates {*zonghe yiti*} the protected information environment and information systems (including military and non-military information systems) and the installations, and put the emphasis on analyzing the dependence and vulnerability {*yisunxing*} of the joint operation's various phases on the information environment. On the basis of conducting the vulnerability analysis and evaluation appraisal, he applies the rules {*fagui*} and various security management measures to implement effective protection of the information environment. The protection of the information environment should include carrying out planning with protection of information sources as its basis. The information's value undergoes changes following on its [use] in the different phases of military activities, and this value should be the basis for determining the information which must be protected and the protection standards. This [determination] reflects the changes in the information value during the different operational phases, and is included within the protection of the information environment.

2. Information attack detection

Information attack detection is the swift discovery of the type {*leixing*} of information attack and its degree of harm {*weihai chengdu*} to friendly information and information systems, to provide a basis for implementing defense. The US military holds that timely and reliable information attack detection is the key to enabling information capability restoration and to effecting rapid response to the enemy attack. The content of information attack detection mainly includes the following: all services' IW centers will receive and issue alerts {*jingbao*} about friendly computer networks suffering attacks, plus prepare and implement technical responses, and prepare and issue analysis reports;

information system developers {*kaifazhe*} should, during design and development {*yanzhi*} of automated information systems, design a variety of security measures; information system providers {*tigongzhe*} and system management personnel should establish a set of management procedures {*guanli chengxu*}, regularly carry out risk assessment and detection {*fengxian pinggu yu jiance*}, be able to timely identify anomalies arising within system functions, and adopt the corresponding measures to reduce the influence produced by the enemy attack; and information and information systems users {*shiyongzhe*} should be able to understand the information systems' own inherent weak links, and be able to carry out identification of anomalous incidents {*yichang shijian*} and of unexplained information alteration {*xinxi genggai*}, as well as of jamming information {*ganrao xinxi*}. **[end of page 409]**

3. Information attack response

Information attack response indicates the responsive activities adopted by the US military after friendly information systems suffer an enemy attack. The US military requires that after encountering an enemy attack, one should timely identify the information attacker {*gongjizhe*}, ascertain his/their intention, and, based on the nature of the information attacker's activities, adopt responsive activities. The options {*xuanxiang*} for responsive activities mainly include legal compulsion {*falyu qiangzhi*}, diplomatic activity, economic sanctions, and military activities. Of these, the military activities on the battlefield include the use of soft and hard kill means, and direct elimination or interruption of the means or systems which the enemy uses to conduct IO.

4. Information capability restoration

Information capability restoration signifies activities in which the US military, after its information systems suffer an enemy attack, relies on already established programs/procedures {*chengxu*} and mechanisms {*jizhi*} to restore the systems' basic functions according to priority level {*youxian dengji*}. The US military's restoration of the information systems' basic functions mainly is done by or at the computer contingency response teams {*jisuanji yingji fanying xiaozu*} and [/or] security incident response centers {*anquan shijian fanying zhongxin*} established by DoD and the various services. They have developed avenues such as automated intrusion detection systems {*zidong ruqin jiance xitong*}, which boost rapid recovery capability after information systems suffer an attack.

IV. IO capabilities of the US military…410

Under the pulling of IO theory, the US military over recent years has annually increased the funds invested in IO weapons and equipment {*wuqi zhuangbei*}, adjusted and built an organizational structure {*bianzhi*} for IO forces in the units of its various services and arms {*ge junbingzhong*}, issued guidelines {*gangyao*} and regulations {*tiaoling*} adapted to IO, conducted IO training and exercises, and formed a fairly strong IO capability.

(1) Electronic warfare capabilities

The organizational structure and equipment of America's various services include almost 600 types of EW systems. These have formed a 3-dimensional [3-D] momentum disposition {*liti bushi*} of ground EW systems, shipborne and airborne EW systems {*jianzai he jizai dianzizhan xitong*}, and EW aircraft (including EW unmanned aerial vehicles [UAVs] {*dianzizhan wurenji*} and EW helicopters), and an EW capability which fuses electronic attack, electronic protection, and EW support [ESM] into an organic whole {*yiti*}. **[end of page 410]**

1. Army EW capabilities

The US Army's organizational structure and equipment include 10-some models and series {*xinghao xilie*} of HF/VHF communication reconnaissance equipment {*tongxin zhencha shebei*}; airborne SIGINT interception {*jizai xinhao qingbao jiehuo*}, positioning, classification {*fenlei*}, and transmission equipment; tactical communication jamming equipment; airborne communication signal direction-finding, interception, and jamming equipment; airborne non-communication radiation source positioning and identification equipment; radar and navigation signal {*daohang xinhao*} automatic positioning and identification equipment; helicopter airborne radar jamming equipment {*zhishengji jizai leida ganrao shebei*}; and laser and radar warning and infrared [IR] jamming {*jiguang he leida gaojing, hongwai ganrao*} systems and equipment {*zhuangbei*}. The performance of all these systems is fairly high. For example, the "Guardrail" {"护栏" *"hulan"*} system has a reconnaissance range {*zhencha juli*} of up to 130 kilometers [km], a communication reconnaissance frequency {*tongxin zhenpin*} of 2-500 MHz, a radar reconnaissance frequency {*leida zhenpin*} of 0.8-12 GHz, a positioning error {*dingwei wucha*} of 50-100m at 100 km, a reconnaissance capability of 20-30 targets/minute for VHF/UHF {*shengaopin/ chaogaopin*} communication, and a reconnaissance capability of 2 targets/minute for HF communication. In addition, the Army ground electronic reconnaissance system frequency has already expanded to 0.5-40 GHz, the radar jamming system frequency range {*pinlyu fanwei*} has reached 8-20 GHz, and jamming power has already reached 4kW; jamming capability is dual-mode {*shuangmo*}, able to jam the enemy's voice communication, data communication, and weapons guidance radar {*wuqi zhidao leida*}; [and the systems] have the capability within the entire EM spectrum range to conduct effective reconnaissance and detection {*zhence*}, monitoring {*jianting*}, recording, analysis, and jamming of the operations zone.

(i) Corps {*jun*} EW capabilities

The US Army's corps organizational system {*jun jianzhi*} internally is organized with military intelligence brigades and combat aviation brigades [among others]. Its EW missions mainly are to acquire EW intelligence, and to perform posture analysis {*taishi fenxi*} and target research and discrimination {目标研判 *mubiao yanpan*}, to meet the intelligence requirements of the corps and its subordinate divisions, independent

brigades, and armored cavalry regiments. Its electronic jamming equipment mostly is forward deployed {*kaoqian bushu*}, and used for supporting the EW activity of the subordinate units.

The EW systems in the equipment of the corps' military intelligence brigades and combat aviation brigades are mainly used for reconnaissance and detection and jamming of enemy communication and radar, as well as [enemy] IR and optical battlefield reconnaissance equipment, and can be installed in ground vehicles and in aircraft. They mainly include ground and airborne communication and **[end of page 411]** radar reconnaissance systems. Their ground communication and non-communication interception range {截收范围 *jieshou fanwei*} is 20 km, and their air communication and non-communication interception range can be as much as 100 km or more. The ground and airborne communication and radar jamming systems have a communication jamming range {*ganrao juli*} of 30 km, and an aerial jamming range of up to 100 km. They can unfold {*zhankai*} 80-90 radio intercept posts {*wuxiandian zhenting shao*} and direction-finding posts {*cexiang shao*} (of which 37-44 are aviation posts {*hangkong shao*}), 12 radio reconnaissance and radio technique reconnaissance posts {*wuxiandian jishu zhencha shao*} (of which 2 are aviation posts), and 14-18 radar and photographic reconnaissance stations {*zhaoxiang zhencha zhan*}. These can conduct regular surveillance of 30-100 shortwave radio nets {*duanbo wuxiandian wang*}, 75-100 ultra-shortwave [USW] radio nets {*chaoduanbo wuxiandian wang*}, 400-512 radio relay communication channels {*wuxiandian jieli tongxin tongdao*}, and 110-120 radar sets. Within 1 hour, they can determine {*ceding*} the coordinates {*zuobiao*} of 400-420 shortwave radio transceivers and 200-240 USW radio transceivers, as well as the coordinates of 25-30 radar sets. A single sortie {*chudong*} of a reconnaissance aerial vehicle {*zhenchaji*} can detect 33-55 targets, and carry out photographing of them. In a corps assigned to offense {*danren jingong*}, the density of its frontal technical reconnaissance instrument equipment {*zhengmian jishu zhencha qicai*} can reach 10-15 stations per km. This [equipment] can conduct surveillance of the deep targets {*zongshen mubiao*} of a defending enemy; of these, for targets within 10 km from the enemy's defensive forward edge {*fangyu qianyan*}, it can carry out 3-5 overlapping coverage reconnaissance {*chongdie fugai zhencha*} [runs].

(ii) Division EW capabilities

The US Army's division organizational structure {*bianzhi*} has military intelligence battalions and combat aviation brigades [as published; evidently "battalions"]. Their EW missions have equal emphasis on reconnaissance and jamming {*zhencha yu ganrao bingzhong*}, to support the division's operational activities. The EW systems in the equipment of the division-subordinate military intelligence battalions and combat aviation brigades [i.e., battalions] are used for reconnaissance and detection and jamming of enemy communication equipment and gun position target search radar {*paowei zhencha leida*}, as well as IR and optical battlefield reconnaissance equipment, and can be installed in ground vehicles and aircraft. They mainly include ground and airborne communication reconnaissance systems, ground and airborne radar EW

reconnaissance systems, and portable communication direction-finding units {*bianxieshi tongxin cexiang ji*}, with a communication interception range {截收距离 *jieshou juli*} of 20 km, and an aerial communication and non-communication interception range of up to 40 km. The ground and airborne communication jamming systems have a communication jamming range of 30 km, and an aerial jamming range of up to 40 km. These battalions, complemented by attached elements {*peishu fendui*}, can unfold 35 **[end of page 412]** radio intercept posts and direction-finding posts, and conduct surveillance on 40-50 radio nets and 15 radar sets, and can determine the coordinates of 60-80 shortwave transceivers, 350-400 USW transceivers, and 24-30 ground radar sets. They can simultaneously suppress 30 radio nets and 10-15 radar sets, and can dispatch reconnaissance teams into a 300-400 km depth.

(iii) EW capabilities of independent brigades and armored cavalry regiments

The Army's independent brigades and armored cavalry regiments are organizationally structured with military intelligence companies. These companies provide the brigade (regiment) commanders with the necessary intelligence, OPSEC support, and jamming of enemy communication and non-communication electronic equipment. The EW systems in these companies' equipment can be installed in ground vehicles or in aircraft. They mainly include ground communication reconnaissance systems, with a communication interception range of 25 km, and a non-communication interception range within 20 km. The ground and airborne communication EW systems have a communication jamming range of 30 km and an aerial jamming range of up to 40 km.

2. Navy EW capabilities

US Navy EW building got started fairly early. Navy airborne EW systems currently include equipment such as an airborne threat warning {*jizai weixie gaojing*} series, a tactical jamming series, a deceptive electronic jamming {*qipian dianzi ganrao*} series, and various types of chaff dispensers {*ganraowu toufangqi*}. Shipborne EW systems can resist radar-guided weapons {*leida zhidao wuqi*}, collect enemy intelligence, and disrupt the enemy radar's normal operation. Their EW capability not only can ensure the needs and requirements {*xuyao*} of aircraft carrier formation naval operations {*hangmu biandui haishang zuozhan*}, but also can extend onto land, to directly support Air Force and Army operations.

(i) EW capabilities of naval aviation forces {*haijun hangkongbing*}

Operational capability {*zuozhan nengli*} of electronic reconnaissance aerial vehicles {*dianzi zhenchaji*}: US naval aviation forces are equipped with EP-3E "Orion" {*"liehuzuo"*} electronic reconnaissance aircraft, RF-4B "Phantom" {*"guiguai"*} reconnaissance aircraft, and EA-6B "Prowler" {*"paihuaizhe"*} EW aircraft. Of these, the EP-3E's main EW equipment is as follows: an instantaneous frequency measurement system {*shunshi cepin xitong*}, electronic support receiver system, radar signal collection

system, multi-purpose radio/wireless communication intercept and analysis system {*duoyongtu wuxiandian tongxin jieshou he fenxi xitong*}, IR warning **[end of page 413]** system, IR pod {*hongwai diaocang*}, reconnaissance direction finding system {*zhencha cexiang xitong*}, and clutter jamming pod {*zabo ganrao diaocang*} (1-3 cm waveband). It can automatically carry out frequency measurement, rapid direction finding, and measurement {*ceding*} of radar signal parameters {*canshu*}; it can identify the radiation sources for various types of radar signals, and determine their location, with a direction-finding accuracy {*cexiang jingdu*} of ±1º; and it can carry out interception, measurement, and recording of radio/wireless communication signals. The main EW equipment of the RF-4B reconnaissance aircraft is as follows: a tactical electronic reconnaissance system, radar warning system, and IR reconnaissance system, as well as a side looking radar {*ceshi leida*}, terrain tracking/surveying and mapping radar {*dixing genzong/cehui leida*}, and Doppler navigation equipment {*duopule daohang shebei*}. The main EW equipment of the EA-6B "Prowler" is as follows: integrated receiving equipment {综合接收设备 *zonghe jieshou shebei*}, threat warning control system {*weixie jingjie kongzhi xitong*}, tactical jamming system, deceptive electronic jamming system {*qipianxing dianzi ganrao xitong*}, continuous-wave [CW] jammer {*lianxu bo ganraoji*}, chaff dispenser, and high-speed anti-radiation missiles [HARMs] {*gaosu fanfushe daodan*}. Its electronic reconnaissance capability is A-J frequency band {*pinduan*} (roughly 0.01-2 GHz), with simultaneous identification of 15 threat targets; the clutter jamming band is 64 MHz – 1.8 GHz (excluding 270-500 MHz), with a jamming power density {*ganrao gonglyu midu*} of 1kW/MHz, and capability for simultaneous dealing with multiple threat targets; the deceptive jamming band is 0.2-2 GHz, capable of covering the entire threat spectrum; pulse jamming power {*maichong ganrao gonglyu*} is greater than 1kW, with a jamming beamwidth {*ganrao boshu kuandu*} of 60º; response time is 0.1 microsecond [μs]; and the communication jamming band is 100-300 MHz or wider.

Operational capability of early warning aircraft: US Navy early warning aircraft mainly include the E-2C "Hawkeye early warning aircraft" {"鹰眼预警机" *"yingyan yujingji"*}. This aircraft is equipped with an electronic support [ESM] system, EW pod, and early warning radar {*yujing leida*}, as well as data processing equipment. Its electronic reconnaissance band is 0.05-1.8 GHz, with capability over a 360º scope for swiftly detecting radar signals being transmitted within the above band, and with an interception range of up to 900 km. This aircraft model, within a space with a radius of several hundred km and an altitude under 3 km, can simultaneously detect, identify, track, and surveil 250 or more various types of targets moving at different speeds. When conducting airborne warning {*kongzhong jingjie*} at 370 km in front of an aircraft carrier {*hangkong mujian*}, via data link {*shuju lian*} and communication equipment, it can timely provide the aircraft carrier battle group [CVBG] {*hangmu zhandouqun*} with **[end of page 414]** target coordinates, batches {*pici*}, and routes, plus their main parameters, for the following: enemy high-altitude bombers {*gaokong hongzhaji*} at 1111 km in the incoming direction from the carrier, low-altitude bombers at 833 km, low-altitude combat aircraft at 788 km, enemy ships {*jianchuan*} at 730 km, and low-altitude cruise missiles {*dikong xunhang daodan*} at 639 km.

Operational capability of patrol aircraft: US Navy patrol aircraft mainly include the P-3C "Orion" anti-submarine patrol and ELINT aircraft {*fanqian xunluo yu dianzi qingbao feiji*} and the ES-3A "Viking" {*"beiou haidao"*} electronic patrol aircraft. Of these, the P-3C's main EW equipment is as follows: an instantaneous frequency measurement system, electronic support [ESM] system, radar warning and surveillance system {*leida gaojing he jianshi xitong*}, tactical electronic reconnaissance system, forward-looking infrared [FLIR] reconnaissance {*qianshi hongwei zhencha*} warning and surveillance system, pulse analyzer {*maichong fenxiyi*}, and surface search radar {*shuimian sousuo leida*}. The radar warning and surveillance system has an operating frequency of 0.02-2 GHz; can conduct surveillance over a 360º azimuth {*fangwei*} and a look-down space {*fushi…kongjian*} of ±45º, with a direction-finding accuracy of better than 15º; and has a threat database {*weixie shujuku*} with the parameters of more than 100 radiation sources, and capability for simultaneously displaying the main technical parameters of 15 radiation sources on the display. The ES-3A's main EW equipment includes a tactical signal exploitation system {*zhanshu xinhao liyong xitong*}, electronic support [ESM] system, chaff dispenser, and warning/search radar. Its reconnaissance wave band is the E-J band, 0.2-2 GHz. Besides executing electronic reconnaissance missions, it also can carry out tracking of submarines.

(ii) EW capabilities of operational ships {*zuozhan jianting*}

The EW equipment of US Navy operational ships takes electronic reconnaissance (warning) and active jamming equipment {*zhudongshi ganrao shebei*} as primary, with passive jamming instrument equipment {*wuyuan ganrao qicai*} as auxiliary (the radar cross section [RCS] {*leida fanshe jiemianji*} of heavy ships {*daxing jianting*}) is roughly 100-6000 m^2, and dispensing of chaff {*toufang botiao*} or IR decoys {*hongwai youer*} requires a maximum dispersal quantity {*sanbuliang*}). The Navy attaches importance to boosting the jam-resistance capability {*kangganrao nengli*} of all types of shipborne radar {*jianzai leida*}.

Aircraft carriers: Conventionally powered carriers {*changgui dongli hangkong mujian*} all are equipped with passive detection equipment {*wuyuan tance shebei*}, instantaneous frequency measurement receivers, and active and passive jamming equipment {*youyuan yu wuyuan ganrao shebei*}. The passive detection coverage frequency is 40 MHz – 0.2 GHz, which not only can conduct communication reconnaissance, but also can conduct radar reconnaissance; the instantaneous frequency measurement receivers are used for detecting and rapidly analyzing threats from anti-ship missiles {*fanjian dandao*},**[end of page 415]** and have a signal intercept rate {*xinhao jiehuolyu*} of 100% within the 0.7-1.8 GHz range. Nuclear powered carriers {*he dongli hangkong mujian*} mainly are equipped with high-power deception jammers and EW surveillance receiver systems. The high-power deception jammers operate within an intensive {*miji*} EM environment, and can monitor and track {*jiance genzong*} signals from multiple types of missiles; the EW surveillance receiver systems can automatically measure the signals' direction of arrival, and carry out classification and identification of

the signals, and can conduct analysis of the signal parameters, plus carry out key point search {*zhongdian sousuo*} for specific frequency bands.

Cruisers and battleships: These mainly are equipped with AN/SLQ-32(V)3 EW systems and MK36 passive jamming transmitter systems {*wuyuan ganrao fashe xitong*}. Their EW systems are mainly used for defense against winged-type missile {*feihangshi daodan*} attacks; can carry out warning and identification of, and direction determination {*ceding*} for radar-guided anti-ship missiles; and have active jamming capability, enabling simultaneous jamming of 80 radar sets. They also can be used for controlling passive jamming system transmissions. Some cruisers and battleships are equipped with towed sonar decoy systems {*tuoyeshi shengna you'er xitong*}; these can detect enemy sonar signals or various parameters of torpedoes.

Destroyers and frigates [escort vessels]: These are equipped with AN/SLQ(V)2 EW systems and MK36 passive jamming transmitter systems. Their EW systems can carry out warning {*baojing*} and identification of incoming radar-guided anti-ship missiles, and can determine their direction. They also can guide {*yindao*} the passive jamming systems' launch of chaff or IR jamming projectiles {*ganraodan*}.

Amphibious operational ships {*liangqi zuozhanjian*} and missile patrol boats {*daodan xunluo ting*}: These are equipped with EW systems and passive jamming transmitter systems.

Submarines: These mainly are equipped with EW surveillance receiver systems, low-frequency [LF] acoustic echo repeaters {*dipin huisheng chongfaqi*}, and HF acoustic echo repeaters. These two types of acoustic echo repeaters both are floating type {*piaofushi*}; when they are irradiated by active sonar, or receive signals transmitted by underwater weaponry {*shuizhong bingqi*} active or acoustic homing systems {声自寻的系统 *sheng zixundi xitong*}, they can repeat the echoes, to achieve confusing the genuine with the spurious {以假乱真 *yijia luanzhen*}, and luring threats toward a false target. Besides the above EW equipment, the US Navy's main operational ships also are universally equipped with EW equipment such as communication jammers and communication direction-finding equipment. **[end of page 416]**

(iii) EW capabilities of the Marine Corps

The USMC has an independent organizational SoS {*zuzhi tixi*}; it can both assist the other services' operations, and also can independently carry out operational missions {*zuozhan renwu*}. The Marine Corps, according to the nature of its main mission, to carry out landing operations {*denglu zuozhan*} and on-island operations {*daoshang zuozhan*}, develops EW capabilities mutually consistent with its mission. Its main EW equipment and capabilities are as follows: the AN/PRD-12 "Top Hunter" {*"gaoji lieshou"*} radio direction-finding system {*wuxiandian dingxiang xitong*}, which can perform interception {*jiehuo*}, surveillance, and positioning of targets, with a direction-finding error of less than 3º (RMS value). The AN/TLQ-17A ["TRAFFICJAM"] communication jamming

system has a frequency coverage range of 1.5-80 MHz, CW jamming power of 550W, and pulse jamming power of 2.5kW; has complete remote control capability; offers search and lock-on {*sousuo suoding*}, priority lock-on {*youxian suoding*}, auto-surveillance {*zidong jianshi*}, band-selectable scanning {*pinduan xuanze saomiao*}, and full-band scanning {*quanpinduan saomiao*} operating modes; and can within 1 second, from among 256 pre-selected frequency bands, tune and align {*tiaoxie duizhun*} any one target needing to be jammed. The AN/MLQ-36 mobile EW support system {*jidong dianzizhan zhiyuan xitong*} is installed in amphibious lightweight armored vehicles {*liangqi qingxing zhuangjiache*}, has an operating band of 20-80 MHz and effective radiated power [ERP] {*youxiao fushe gonglyu*} of 400W, and can discharge suppressive and deceptive jamming {*yazhixing he qipianxing ganrao*}. It has automatic intercept {*zidong jiehuo*} and threat assessment {*weixie panduan*} capabilities, and the capability for performing jamming; and within 1 second, it can from among 16 preset target channels, select one or more having a high threat level, to conduct the jamming. It also can per a program {*chengxu*} conduct jamming of specific bands and predetermined signals. In addition, [USMC] also has EW equipment such as vehicle-mounted/airborne ground tactical communication jamming centers {*chezai/jizai dimian zhanshu tongxin ganrao zhongxin*} or positioning and warning systems {*dingwei jingjie xitong*}, portable/airborne {*shouti/jizai*} HF communication jamming [systems], and identification friend or foe [IFF] systems {*diwo shibie xitong*}.

3. EW capabilities of the Air Force

The USAF is, among all the services, the service with the strongest EW capability. Its airborne jamming equipment has a frequency band which has already expanded to 64 MHz – 18 GHz, and a jamming ERP already reaching 1MW. Its airborne electronic reconnaissance systems have the capability for detecting and intercepting a variety of EM-radiation signals of the enemy; can provide the location, nature, activity situation, and threat level of radiation sources; and have an intelligence reconnaissance receiver frequency {*qingbao zhencha jieshouji pinlyu*} which has already expanded to 0.03-40 GHz. Its radar **[end of page 417]** warning systems have a frequency coverage range which generally already can reach 0.5-18 GHz, a probability of intercept {*jiehuo gailyu*} which can reach 100%, and the ability to vector ARMs to attack targets. Its radar jamming systems have a jamming frequency coverage range which generally can reach 0.5-20 GHz, and a maximum jamming power density which can reach 1kW/MHz; one jammer can simultaneously jam tens of radar sets. Its airborne electro-optical [E-O] reconnaissance and detection systems {*jizai guangdian zhence xitong*} have the capability to operate under a variety of EM jamming conditions; and the airborne E-O weapons systems have the capability for target acquisition {*mubiao buhuo*}, tracking, identification, and measurement {*celiang*}, plus the capability for attacks on targets.

(i) Electronic reconnaissance capabilities

USAF electronic reconnaissance aircraft are divided into strategic electronic reconnaissance aircraft and tactical electronic reconnaissance aircraft. The strategic

electronic reconnaissance aircraft mainly include the RC-135, SR-71, and TR-1A [models], while the tactical electronic reconnaissance aircraft mainly include the RF-4C model. The RC-135 reconnaissance aircraft is equipped with EW reconnaissance and jamming equipment such as a reconnaissance receiver, ELINT system, ELINT rapid scanning receiving equipment, a pulse analysis and direction-finding unit {*maichong fenxi cexiang ji*}, and a clutter jammer {*zabo ganraoji*}. This aircraft model is mainly used for fulfilling strategic reconnaissance {*zhanlue zhencha*} missions; it collects data and radiation intelligence {*fushe qingbao*} on radar characteristics {*leida xingneng*}, guidance systems {*zhidao xitong*}, and communication (including detection and analysis of RF radiation {*shepin fushe*} coming from power lines and transport motor vehicles {*yunshu qiche*}), but does not directly penetrate {*tupo*} the enemy air zone {*kongyu*}. The TR-1A reconnaissance aircraft is equipped with synthetic aperture side-looking radar {*hecheng kongjing ceshi leida*} and a variety of electronic reconnaissance devices. Over the operations zone, it can carry out day/night continuous high-altitude, all-weather, long-distance {*yuanjuli*} reconnaissance and surveillance [R&S]; can conduct reconnaissance of ELINT beyond 55 km in the enemy depth {*zongshen*}; and is mainly used for providing direct support to ground and air units. This aircraft model also is used as a precision positioning attack system {*jingque dingwei gongji xitong*}; it can accurately determine the location of enemy radar-controlled air defense weapons {*fangkong wuqi*} and important installations, and vector attack aircraft or missiles and bombs to execute attacks against the accurately determined locations, so as to destroy the enemy air defense weapon systems. The RF-4C reconnaissance aircraft is equipped with a tactical electronic reconnaissance system, radar homing and warning system {雷达寻的和警戒系统 *leida xundi he jingjie xitong*}, ELINT system, dual-mode jamming pod, and other equipment. Its main missions are to detect {*zhence*} and record the enemy's "electronic combat sequence" {*"dianzi zhandou xulie"*}; **[end of page 418]** in real time, to detect {*tance*} and provide the precise locations of important threat transmitting sources {*weixie fasheyuan*}; to provide short-distance and long-distance related data; to provide immediate warning, positioning, and threat type information for attack aircraft escort {*huhang*}; and to swiftly make battlefield combat damage assessments {*zhanchang zhandou huishang de pingjia*}. The airborne part operates in concert {*peihe*} with a ground threat processing center, and can provide tactical commanders at all levels with the necessary intelligence.

(ii) Electronic jamming and anti-radar capabilities

USAF electronic jamming aircraft mainly include the EF-111A model and EC-130H model. The EF-111A electronic jamming aircraft is equipped with such EW equipment as a tactical electronic jamming system, deception jamming system, radar warning system, chaff dispensing system, and digital computer. Its jamming frequency is 30 MHz – 1.8 GHz, and the output power of each jammer (total of 10 on the plane) is almost 2kW. This aircraft is currently the world's only electronic jamming aircraft which can execute three types of missions: long-distance jamming, escort jamming {*bansui ganrao*}, and short-distance air support. The EC-130H aircraft is a high-power electronic jamming aircraft; it is equipped with an electronic jamming system used for conducting

jamming against enemy equipment such as radio/wireless communication and C2 systems, as well as missiles, and has a very strong jamming suppression [blanket] {*ganrao yazhi*} capability. This aircraft also is equipped with a radar warning receiver, IR reconnaissance system, and other electronic equipment. The F-4G "Wild Weasel" {*"ye youshu"*} aircraft is an anti-radar attack type EW aircraft {*fanleida gongjixing dianzizhan feiji*} which combines radar, navigation, and display electronic systems with attack weapons systems such as ARMs into an organic integrated whole {*youji zhengti*}; which can precision position radiation sources, and use ARMs to destroy them; and which carries out "hard" kill against enemy radar and other air defense equipment. It is equipped with a radar homing and warning {*jingjie*} system, radar warning {*gaojing*} system, dual-mode jamming pod, chaff and flare dispensing system {*botiao he shanguangdan toufang xitong*}, and other electrical equipment. This aircraft uses anti-radar missiles as its main weapons, the commonly used ones including the "Shrike" {*"baisheniao"*} ARM, "Standard" {*"biaozhun"*} ARM, and the "HARM" {*"hamu"*} [high-speed] ARM. During operational employment, this type of aircraft goes ahead of friendly attack aircraft, or together with attack aircraft [flies in] mixed formation {*hunhe biandui*} deep into the threat scope of the enemy air defense system, and specially **[end of page 419]** suppresses and [/or] destroys the enemy air defense radar positions {*fangkong leida zhendi*}, or it indicates {*zhishi*} the enemy radar locations for other friendly attack aircraft, to create the conditions for the activities of the follow-up attack aircraft groupings {*houxu gongjiji qun*}.

(iii) Electronic self-defense capabilities {*dianzi ziwei nengli*} of operational aircraft

All USAF operational aircraft are outfitted with self-defense EW equipment {*ziweixing dianzizhan zhuangbei*}. At present, the various types of EW equipment already fielded total more than 200 types, which mostly can be divided into three basic types: airborne reconnaissance and warning equipment {*jizai zhencha gaojing shebei*}, active jamming equipment {*youyuan ganrao shebei*}, and passive jamming equipment {*wuyuan ganrao shebei*}. In addition, [all aircraft] are also equipped with other electronic equipment closely associated {*miqie xiangguan*} with EW, such as airborne radar, communication, navigation, and identification systems. Along with the airborne EW equipment, these compose an organic integrated whole, which supports {*baozhang*} the operational aircraft's operations, in all weather, at high altitudes, and over long and short distances, against the different air, ground, and sea targets.

The USAF, while placing key points on developing radar EW equipment and systems, also pays unusual attention to developing EW equipment for communication EW and E-O EW. Its communication EW equipment includes two types — airborne equipment and ground base installations {*dimian jidi sheshi*} — and can carry out barrage, spot, responsive, and deceptive jamming {*zuseshi, miaozhunshi, yingdashi, qipianshi deng ganrao*}.

(2) Computer network operations capabilities

The US military has network resources superiority and advanced IT, and regards CNO as a strategic means to be given a high degree of attention. In recent years, it has formulated complete computer network security plans {*jisuanji wangluo anquan guihua*}; researched and developed {*yanzhi he fazhan*} means such as program presets {*chengxu yuzhi*}, chip weapons {*xinpian wuqi*}, and injection of viruses; and formed a fairly powerful CNO capability.

1. Formulation of complete network security plans {*wangluo anquan jihua*}

Under the guidance of DoD's unified information systems security planning {*guihua*}, all US military services one after another have formulated service information system security plans {*jihua*}. The Army in 2000 began implementing its network security improvement plan. The first phase of this plan is to improve network surveillance {*wangluo jianshi*}, intrusion detection {*ruqin zhence*}, and response techniques; the second phase is to open-up develop [exploit] {*kaifa*} several specific techniques; the third phase is to establish a secure connection network {*anquan de lianjie wangluo*} between the master station {*zongzhan*} and its external field equipment {*waichang shebei*}; and the fourth phase **[end of page 420]** is to have all users enter the network from 4 network security portals {*wangluo anquan rukou*}. The Navy decided to use smart card technology {*zhineng ka jishu*} to inspect {*jiancha*} the "identity" {*"shenfen"*} of users entering the secure network. It is currently setting about building 9 large-scale networks (5 on the homeland {*bentu*} and 4 overseas), and all these networks will use this smart card technology to ensure the security of the networks. The Air Force is now developing {*yanzhi*} and verifying {*yanzheng*} a system to detect radio-frequency link intrusions {*wuxiandian pinlyu lianlu ruqin*}, to be used as an intelligent software tool {*zhineng ruanjian gongju*} for surveillance of non-secure and non-sensitive {*feibaomi bumingan*} information network addresses {*xinxi wangzhi*}, and used as automated equipment for surveillance of non-secure telephone and e-mail information.

2. Establishment and building {*zujian*} of network security institutions {*jigou*} and units {*budui*}

In order to boost CNO capability, the US military, while formulating information system security plans {*jihua*} at all levels, is energetically establishing and building network security institutions and units. In the Pacific Theater, Europe, and Arizona, the Army already has established area-wide network activities centers {*duquxing de wangluo xingdong zhongxin*} and computer contingency incident response teams {*jisuanji yingji shijian fanying xiaozu*}, in order to protect and operate {*caozong*} networks in specific areas {*teding diqu*}. The Air Force has organizationally structured {*bianzhi*} network warfare [CNO] detachments {*wangluozhan fendui*} at all of the following: Ninth Air Force at [Shaw] Air Force Base [AFB] in South Carolina, Air Force HQ {*silingbu*} [i.e., "Network Integration Center"] at Scott AFB in Illinois, USAF Seventh Air Force at Osan {乌山} Air Base in South Korea, United States Air Forces in Europe [USAFE] at

Ramstein Air Base in Germany, Pacific Air Forces [PACAF] at Hickam Air Base in Hawaii, and Eighth Air Force at Barksdale AFB in Louisiana, as well as Twelfth Air Force at Davis-Monthan AFB in Arizona. Moreover, US Space Command [USSPACECOM] {*meiguo hangtian silingbu*} in 2000 established and built a regular joint task force {*zhenggui de lianhe teqiandui*}, responsible for dealing with computer network attacks. The Navy, as far back as October 1995, activated the Navy Information Operations Center at Norfolk [naval base] in Virginia.

(3) PSYOP capabilities

The US military's PSYOP strengths come under the jurisdiction {*guishu*} of special operations forces {*tezhong zuozhan budui*}. The Army has organized PSYOP groups {*dadui*} and Reserve PSYOP groups, but the Navy and Air Force only have a small number of PSYOP units. The Army's 4th PSYOP Group is the US military's only active-duty PSYOP unit. This unit **[end of page 421]** dispatched to forward-edge areas {*qianyan diqu*} 4 forward support detachments {*qianyan zhiyuan fendui*}, 2 of which are in the Asian-Pacific area (respectively at Pacific Command [PACOM] {*taipingyang zongbu*} and at US Forces, Korea [USFK] Joint HQ {*zhuhan lianhe budui silingbu*}). The Air Force is equipped with a number of EC-130E PSYOP aircraft and a number of MC-130 aircraft. The EC-130E aircraft mainly execute missions to broadcast FM and AM radio programs, as well as TV programs, while the MC-130 aircraft are used for disseminating leaflets. The US military mainly adopts modes such as battlefield radio broadcasting, dissemination of leaflets, media propaganda, sending of e-mail, and direct telecom {*dianxun zhida*} to carry out PSYOP, including psychological attack {*gongxin*} propaganda, awing [frightening] of the will {*yizhi zhenshe*}, influencing of emotions, and psychological deception {*xinzhi qipian*}, against the enemy. From the viewpoint of several recent local wars, the US military possesses a fairly strong PSYOP capability. During the Kosovo War, less than 1 week after the air raids commenced, 6 EC-130E PSYOP aircraft of the USAF 193rd Special Operations Wing {*tezhong zuozhan liandui*} began to take to the air in turns {*lunliu shangkong*}, and every day transmitted 4 hours of radio and TV programs within the territory of the Federal Republic of Yugoslavia [FRY] {*nan lianmeng*}, and directly applied the Serbian language to conduct propaganda against FRY officers and men {*guanbing*}. Another PSYOP unit of USAF also successively air-dropped {*kongtou*} tens of millions of intimidating and persuasive {劝降 *quanjiang*} leaflets onto 12 main cities within FRY territory, and effectively eliminated the FRY military's will to resist. During the Iraq War, the US military's PSYOP units employed 58 sorties {*jiaci*} of EC-130E aircraft, conducted 306 hours of radio broadcasts {*diantai boyin*} and 304 hours of TV rebroadcasts, disseminated more than 30 million leaflets in 81 types, and conducted fairly effective psychological attacks against the Iraqi military.

(4) Entity destruction capabilities

Over the past few years, the US military, while developing IO "soft" attack means, has laid stress on the combination of "soft and hard," and energetically developed entity destruction means such as EM pulse bombs [E-bombs] {*dianci maichong zhadan*},

graphite bombs {*shimo zhadan*}, cruise missiles, and ARMs, to boost its integrated capability {*zonghe nengli*} for IO. **[end of page 422]**

Section 2: Information Operations of the Taiwan Military…423

Since the 1990s, Taiwan military thought has undergone major changes. The Taiwan military holds that following on the arrival of the Information Age, future wars will be wars which take information and IO as the lead. The Taiwan military regards IO as an operational pattern of strategic level, and devotes a high degree of attention to the important means for island defense {*haidao fangyu*}. To this end, the Taiwan military in recent years has constantly increased the degree of force {*lidu*} in its IO strength building and training; has drawn up {*niding*} near-term and long-term IO development plans {*jihua*}; and has regarded boosting of the IO capabilities of its Army, Navy, and Air Force as the most important objective of building the military and preparing for war {*jianjun beizhan*}.

The Taiwan military's IO theoretical research and strength building have been developing on the basis of EW theory and strength building. Its understanding [awareness] {*renshi*} of IO conceptions {*gainian*} has gone through a process of gradual deepening; and at present the appellation {*chengwei*} of Taiwan military IO also has multiple formulations, such as "information warfare" {"资讯战" *"zixunzhan"*}, "electronic information operations" {*"dianzi zixun zuozhan"*}, and "information operations" {*"zixun zuozhan"*}.[25]

In the current world military field, only the Taiwan military has put forth the conception of electronic information operations. The Taiwan military holds that electronic IO is an all-new conception formed by combining electronic operations {*dianzi zuozhan*} and IO {*zixun zuozhan*}. As for the reason why the Taiwan military has put forth this conception, it is mainly based on the gradual fusion of electronics, information {*zixun*}, communication, and networks in terms of S&T and application; thus, electronic operations and IO likewise are gradually fusing into an organic whole. In particular, on the occasions when the Taiwan S&T levels {*shuiping*} still show quite a gap from those of the advanced nations of Europe and [North] America, if electronic operations are directly classified within IO, it would be easy to confuse the common masses' understanding of the original electronic operations. Hence, the Taiwan military has proposed that it can, based on its developmental evolution {*yange*} and content, call IO as EW in the broad sense, and call EW as IO in the narrow sense. The operational goal of

[25] Translator's note: *zixun* is a variant form of "information" typically used in Taiwan.

both is then to paralyze the enemy's various types of information systems {*zixun xitong*} and information associated weapons **[end of page 423]** systems.

On the basis of the US military's viewpoints, the Taiwan military defines IO as follows: "Information operations are those which take advantage of opportunities {借 *jie*} to influence the enemy's information and information systems and gain information superiority {*zixun youshi*}, so as to assist-support {*zhiyuan*} national military strategic actions {*guojia junshi zhanlue zuowei*}, and at the same time to protect the security {*anquan*} of our information and information systems." From the Taiwan military's definition of IO, one can see that the Taiwan military regards IO as a strategic-level operational pattern to be given a high degree of attention, and has a full understanding of the position and role {*diwei zuoyong*} of IO within war. It holds that IO has a close relationship to national security; that its scope contains the political, economic, and psychological national information infrastructure {*xinxi jichu jianshe*}, as well as the strategic and tactical military information infrastructure; and that all execution of attacks or protective activities against these infrastructures falls within the category of IO. Below, for convenience in study of the issues, we use *xinxi zuozhan* (IO) for the general term Taiwan military *zixun zuozhan* (IO).

The Taiwan military's classification of IO conceptions on the whole continues to use the US military's classification. According to operational level, it divides IO into two levels: strategic IO and tactical IO; and according to the nature of the activities, it mainly divides it into seven types: C2 operations, intelligence operations, electronic operations, PSYOP {*xinli zuozhan*}, economic IO, [computer] network operations (network intrusion operations {*wangluo ruqin zuozhan*}), and computer hacker operations {*diannao heike zuozhan*} (computer control warfare {*diannao kongzhizhan*}).

I. Basic viewpoints and principles of Taiwan information operations…424

The Taiwan military draws inspiration from the Persian Gulf War and Kosovo War. After having analyzed in manner having a directed [focused] quality {*you zhenduixing di*} the current state {*xianzhuang*} and trends of the mainland's IW, it clearly pointed out that it will at the beginning of the 21st century activate an "intimidating EW superiority combat power" {*"xiazuxing dianzizhan youshi zhanli"*} having both attack and defense {*gongshou zhanbei*} [capability], to contend for information dominance {*zhixinxiquan*}. In recent years, the Taiwan military has increased the degree of force in its IO research, and has formed a relatively complete [set of] IO viewpoints.

(1) Basic viewpoints

1. Implementing the IO guidance of the "strategic defensive {*zhanlue shoushi*} and tactical offensive {*zhanshu gongshi*}"

The Taiwan military holds that the mainland in recent years has increased its studies on IO theory, and **[end of page 424]** has renewed its IW equipment {*xinxizhan*

zhuangbei}, and already possesses a fairly strong IO capability. Hence, in terms of IO tactics {*celue*}, it should also consider political needs and requirements, should not excessively reveal its capabilities {*fengmang*}, and should abide by the overall operational requirements {*zongti zuozhan yaoqiu*}, so as to benefit great power support {*daguo zhichi*}. However, in terms of specific IW tactics, it should exploit EW "activities which discover {*chajue*} the enemy's intent, and counter-preempt {*fanzhi*} the enemy," and have EW penetrate through the entire operational process. Hence, it requires that its Air Force should flexibly apply EW aircraft, early warning aircraft, and various other items of electronic equipment; and, based on the integrated-whole operational plan, combined with specific tactical activities, adopt all feasible means to timely conduct electronic suppression against the adversary, to hope for paralyzing or weakening the enemy early warning and command systems, and support {*baozhang*} the execution of operational missions. In wartime, the three services {*sanjun*} should, while doing their utmost to conduct full-dimensional, multilevel, large-depth, uninterrupted {*quanfangwei, duocengci, dazongshen, bujianduan*} information collection against the adversary, also [realize] integrated application {*zonghe yunyong*} of multiple means to continuously carry out electronic suppression and network attacks against the mainland, so as to contend for EM superiority {*dianci youshi*}.

2. Laying stress on "long-range monitoring {*yuancheng jiankong*} and early-stage early warning," and doing everything possible to seize the [advantage of the] operational first opportunity {*zuozhan xianji*}

The Taiwan military holds that Taiwan Island's special geographic location has determined that it must, via "long-range monitoring and early-stage early warning," timely acquire the mainland's seacoast arms movements {*yanhai junbei dongxiang*}, and that only in this manner can it seize the operational first opportunity. On these grounds, the Taiwan military requires that its Air Force should, based on the "Chi'ang Wang" {"强网"} system, build a multilevel, full-dimensional integrated intelligence reporting SoS {*zonghe qingbao baozhi tixi*}; and apply multiple reconnaissance means, such as radar, technical reconnaissance {*jizhen*}, airborne early warning [AEW] {*kongzhong yujing*}, photoreconnaissance {*zhenzhao*}, and reconnaissance patrols {*zhenxun*}, to [conduct] 24-hour, all-weather, full-dimensional, 3-D reconnaissance {*liti zhencha*}, to acquire air intelligence {*kongzhong qingbao*} on the mainland's deep areas. On the ground, its 30-some sets of surface-to-air warning and guidance radar {*duikong jingjie, yindao leida*} should form a circular disposition {*huanxing bushu*} with Taiwan Island as its center and the western part as the key point, and constitute a multilevel, fairly rigorous {*yanmi*} surface-to-air warning net. It requires that the E-2T AEW aircraft {*kongzhong yujingji*} should fly over Taiwan's central mountain range or Taiwan's eastern air zones, and when necessary, maneuver forward {*jidong qianchu*} to the [Taiwan] Strait area {*haixia diqu*}. Their key points are to reinforce {*jiaqiang*} the surveillance search {*jianshi sousuo*} for low-altitude targets, and at the right time take over to make up for {*jieti mibu*} the gaps {*kongxi*} in ground radar coverage. In addition, it also emphasizes the use of technical reconnaissance means to acquire deep-inside-story {*neimuxing qiang*} operational intelligence on the mainland's southeast seacoast first-line unit readiness {*yixian budui*

zhanbei} situation, operational instructions {*zuozhan zhiling*}, and flight forecasts {*feixing yubao*}. It applies **[end of page 425]** RF-5E and RF-16 reconnaissance aircraft, as well as various models of combat aircraft, to conduct aviation reconnaissance point blank {抵近 *dijin*} along the mainland seacoast, and timely grasp the mainland's real strength and organized defenses {*shili bufang*}, as well as important target data {*mubiao ziliao*}. Via the above various long-range monitoring means, it puts key points on grasping the mainland seacoast's air flight dynamic situation {*kongzhong feixing dongtai*}, on surveillance of the mainland's first-line medium- and high-altitude targets {*zhong, gaokong mubiao*} north to the Zhoushan Archipelago [at the mouth of Hangzhou Bay] and south to the southern Penghu Islands [Pescadores] {*nan peng liedao*}, and on grasping all types of aerial targets active in the southeast seacoast areas, in order to provide early-stage early warning for timely implementation of counter-suppression operations {*fanzhi zuozhan*}.

3. Emphasizing "head attacks, with precedence to political ones {*zhengzhi youxian, yuantou gongji*}"

The Taiwan military stresses that IO should implement the principle of "head attacks, with precedence to political ones" in counter-suppression operations. This means that the selection of IO targets should be mutually complementary {相辅相成 *xiangfu xiangcheng*} with counter-suppression operations, and that preliminary information suppression {*xianqi xinxi yazhi*} not only must aim at the adversary's military "point targets" {*"dianzhuang mubiao"*}, but also must lay stress on damaging or disrupting {*huishang, pohuai*} "planar targets" {*"mianzhuang mubiao"*} which have an overall situation {*quanju*} influence on the adversary's campaign activities {*zhanyi xingdong*} and which exert a shocking effect {*zhenhanxing xiaoying*}, and execute "head attacks." On these grounds, the Taiwan military emphasizes, on one hand, that it should adopt the mode of a mutual combination of "soft kill" and "hard destruction" to execute precision strikes {*jingque daji*} on political and economic targets in political and economic center cities such as Xiamen, Shanghai, and Hong Kong, and thus achieve [the goals of] creating an adverse political influence, and shaking the adversary's strategic resolve {*zhanlue juexin*} to attack Taiwan. On the other hand, it should employ a mutual combination of "soft kill" and "hard destruction" to damage command information systems and reconnaissance and intelligence installations, and contain {*ezhi*} the bringing into play of the adversary's high-tech force-strengths and combat power {*bingli zhanli*}. The Taiwan military holds that once the adversary's C3I system goes out of order {*shiling*}, his advanced weapons and equipment then will also be difficult to bring into use and to use well. To this end, the Taiwan military attaches even more importance to adopting "soft kill" and "hard destruction" means to disrupt the adversary's southeast seacoast area command information and reconnaissance and intelligence systems, and during exercises with troops {*shibing yanxi*} it lays stress on carrying out simulated attacks {*moni gongji*} against the correlated targets.

4. Mutually combining "soft kill" and "hard destruction," to seize and maintain local information dominance {*jubu zhixinxiquan*}

The Taiwan military holds that when conducting information suppression, it should take a "combination of soft and hard attacks, **[end of page 426]** to ensure information and electronic superiority {资电优势 *zidian youshi*}" as the principle, to seize and control local EM dominance {*jubu zhidianciquan*}. In wartime, the Taiwan military, while ensuring the capability for conducting full-dimensional, multilevel, large-depth, uninterrupted information acquisition against the mainland, also should adopt the dual tactics {*liangshou*} of "soft kill" and "hard destruction" to conduct information suppression against the mainland, in hopes of contending for information superiority. Its specific considerations are as follows: when the mainland carries out a sea-air blockade {*haikong fengsuo*} and landing preparations {*denglu zhunbei*}, on one hand it will put into action {*chudong*} E-2T and C-130HE EW aircraft to conduct electronic suppression against the mainland southeast seacoast C3I systems; and on the other hand, it will timely acquire the technical parameters of the EM waves and EM spectrum {*dianci pinpu*} radiated by the adversary's C3I systems, and at the right time vector various types of ARMs to execute hard destruction of the targets, in hopes of paralyzing the mainland's reconnaissance and early warning and command communication systems. After the NATO air raids against the FRY, the Taiwan military made it clear that IO with electronic offense {*dianzi jingong*} and electronic suppression {*dianzi yazhi*} as its main content was being added to the list of troop drill and training {*yanxun shibing*} subjects for the next several years' "Han Kuang" {"汉光"} series of exercises.

5. Combining professional and nonprofessional strengths, to conduct information attack and defense operations {*xinxi gongfang zuozhan*}

The Taiwan military stresses that the professional IW units should take implementing of information offensive activities {*xinxi jingong zuozhan*} as primary, while the nonprofessional IW units will take implementing of information defense as the root {*genben*}. On these grounds, its Air Force took the lead in establishing and building "EW air groups" {*"dianzizhan dadui"*}, equipped with E-2T model AEW aircraft and C-130HE model EW aircraft; its Army also is successively augmenting {*kuobian*} the EW companies of its large formations {*juntuan*} into EW battalions; and its Navy already has perfected its shipborne IW equipment. In addition, the Taiwan "Ministry of Defense" has continued to establish "information attack teams" {*"zixun gongji xiaozu"*} and "IW crisis handling centers" {*"zixunzhan weiji chuli zhongxin"*}, respectively arranged fielding {*liezhuang*} of new IW equipment for newly planned and organized {筹组 *chouzu*} professional-quality IO units, and already put them through US military cultivation and training {*peixun*}, so that it now possesses a certain IO capability. The network warfare techniques {*wangluozhan jishu*} it has exploited {*kaifa*} already have the capability for infiltrating and disrupting large-scale Army and civilian computer network systems. The nonprofessional IW units, then, are composed of radar observation and communication units {*leida guantong budui*} and communication and information units {*tongxin zixun budui*} of the Army, Navy, and Air Force; they mainly assume radar and communication

anti-jamming operational missions and computer network security protection missions, so as to support {*baozhang*} the ability of friendly systems to normally operate within EW and network warfare confrontation {*dianzizhan, wangluozhan duikang*}. **[end of page 427]**

In order to boost the operational capability of its IW units, the Taiwan military has already formulated training guidelines for IO. In recent years, during many exercises and training [programs], the Taiwan military has gradually increased the content of IW, so as to boost the units' understanding of IW, and to test {*jianyan*} its real-combat application effects {*shizhan yingying xiaoguo*}. During the "Han Kuang" tri-service joint operations exercises {*sanjun lianhe zuozhan yanxi*} which the Taiwan military holds, it for the first time has added in computer virus, logic bomb, and other network attack content.

(2) Basic principles

Since the 1980s, the Taiwan military, while actively seeking to purchase {*xungou*} US military command information system technology, and concentrating efforts on building complete, stable, high-efficiency information systems, has regarded IO as a key point in armed forces building {*jianjun zhongdian*}, has successively established tri-service professional IW units, and has continued to issue new versions of *Republic of China [ROC] Armed Forces Intelligence Guidelines* {*guojun qingbao gangyao*}, *ROC Armed Forces Communication and Electronics Guidelines* {*guojun tongxin dianzi gangyao*}, and *ROC Armed Forces Electronic Warfare Guidelines* {*guojun dianzizhan gangyao*}.[26] The Taiwan military's IO guidance will abide by the following principles.

1. Unified command {*tongyi zhihui*} and integrated-whole adjusting-coordination {*zhengti xietiao*}

The Taiwan military, having carried out all-around deliberation and evaluation appraisal {*kaoliang pinggu*} of its IO capability, holds that its general operational units' IO capability is fairly weak, and usually is limited to self-protection only. Its professional IW units have an integrated {*wanzheng*} IO capability, but are limited in numbers. The two must be closely combined in order to produce an effective lethal might {*shashang weili*}. Hence, within future anti-landing operations {*fandenglu zuozhan*}, in terms of IO guidance, it should abide by the principle of unified guidance and integrated-whole adjusting-coordination. That is, all unitary, discrete {*danyide, lisande*} information weapons and information systems should be placed under the command and control of unified, large-scale systems, to carry out integrated-quality IW activities {*zonghexing de*

[26] Translator's note: "ROC" is used here for convenience, since the PRC does not use this term.

xinxi duikang xingdong}. On these grounds, on one hand it emphasizes that commanders {*zhihuiguan*} should, under unified planning, combine the application of techniques and tactics, to [implement] unified command of the various types of information strengths. On the other hand, the professional IW units and nonprofessional units should be closely coordinated {*miqie xietong*}, so as to bring into play the united combat power {*tonghe zhanli*} of all types of information systems within new types of military confrontation. Its specific requirements are as follows: "the Heng Shan combat situation information management system {衡山战情资讯管理系统 *hengshan zhanqing zixun guanli xitong*}" should, based on the general operational courses of action [COAs] {*zongti zuozhan fang'an*}, employ multiple communication networks **[end of page 428]** to implement C2 over all services (arms) {*ge jun (bing) zhong*}, the 1st through 5th Theaters {*zhanqu*}, and the Kinmen [Quemoy] and Matsu Defending Forces {*fangwei bu*}, and to unify their IW activities. The Air Force's "Ch'iang Wang" system, the Army's "Lu Tzu" {"陆资"} system, and the Navy's "Ta Ch'eng" {"大成"} system, as well as the Coast Guard's {海巡部 *haixun bu*} "Hai Shen" {"海神"} system, should —under unified command by the "Heng Shan combat situation information management system" — fully bring into play the roles of their respective systems; and, strictly according to the pre-combat drafted {*zhanqian nizhi*} coordinated activities plan {*xietong xingdong jihua*}, ensure accurately implementing integrated {*yitihua*} IW activities in respect to the specified {*guiding*} times, places, content, and methods.

2. Having both offensive and defensive {*gongshou jianbei*} [capability], and using attack to promote defense {*yigong cufang*}

The Taiwan military holds that IO should strictly execute the main idea {要旨 *yaozhi*} of joint operations, and [realize] integrated application of multiple information means to conduct IO activities having both offensive and defensive [capability]. On these grounds, it stresses integrated application of intelligence warfare {*qingbaozhan*}, EW, and CNO, to conduct triadic {*sanwei yiti*} IO activities having both offensive and defensive [capability]. This requires that commanders at all levels should combine the application of information counter-suppression {*xinxi fanzhi*} (i.e., information attack) and information counter-counter-suppression {*xinxi fanfanzhi*} (i.e., information defense); and, while protecting friendly information systems, prevent the normal bringing into play of the adversary's information system functions, to ensure effectively seizing information dominance. The specific requirements for this are as follows: commanders should fully bring into play the professional IW units' operational capability; [realize] integrated application of multiple information counter-suppression means by the professional IW units; and, via a mutual combination of "soft kill" and "hard destruction," flexibly conduct stable, high-efficiency IO activities. The nonprofessional units' information activities should take information counter-counter-suppression as primary, and take ensuring the normal operation {*yunzhuan*} of friendly information systems as the objective. [The Taiwan military] stresses that all levels of commanders, when formulating specific IO activities COAs {*xingdong fang'an*}, should unify the command and control [C2] {*zhihui yu guanzhi*} of the subordinate professional IW units {*danwei*} and information systems, and carefully plan {*cehua*} this. When carrying out

IO activities, they should select favorable time opportunities {时机 *shiji*} and effective means to [achieve] unified assignment of missions {*tongyi fuyu renwu*}, and bring into play the optimal effectiveness of all types of weapons and information systems.

3. Seizing opportunities for combat {*zhanji*}, and rapid response

The Taiwan military stresses that the effects of information counter-suppression are dependent on the seizure of counter-suppression time opportunities and **[end of page 429]** on the capability for rapid response. Overly early implementation will give the enemy the opportunity for effective protection. In particular, since information counter-suppression and intelligence collection are mutually containing {*huyou qianzhi*}, long-term implementation of information counter-suppression will increase the difficulty of intelligence collection. Hence, in order to both benefit intelligence collection and also be able to boost the effects of counter-suppression, commanders at all levels must select the optimal counter-suppression time opportunities. Usually these are as follows: when the enemy command communication is frequent, presaging that major attack activities are about to be launched, they should strengthen intelligence collection, so as to grasp the enemy's intention and activities; when the enemy issues attack orders and moves units {*diaodong budui*}, they should implement information counter-suppression, to corrupt {*raoluan*} the enemy command; and when the enemy weapons systems constitute direct threats to the friendly side, or when the friendly side adopts attack activities, they should implement eruptive {*tufaxing*} electronic counter-suppression {*dianzi fanzhi*} so that the enemy is taken by surprise {措手不及 *cuoshou buji*}, and loses an opportunity for combat.

4. Fully preparing, and gaining victory by stratagem {以谋制胜 *yimou zhisheng*}

The Taiwan military emphasizes that the key to the success or failure of information counter-suppression operations lies in the degree of preparations before combat. The response time of IO under modern conditions is extremely brief, so in peacetime one must do a good job of full preparations. This requires that IO units must accomplish equal emphasis on peacetime and wartime, and often add drills {*yanlian*}, to ensure that in wartime they will be able to swiftly mount a response. In order to obtain preemptive {*xianzhi*} and surprise attack {*qixi*} effects, they should focus on the adversary's weak points, and excel at using electronic stratagems {*dianzi moulue*}, leading to mistakes in the adversary's assessments; select appropriate tactics to cause the adversary to exhibit even more loopholes {*loudong*}; and at the right time [execute] harassing attacks behind enemy lines {*xirao dihou*}, forcing the enemy force-strengths to decentralize {*bingli fensan*}, and fall into passivity {*beidong*}.

II. Information operations strengths of the Taiwan military…430

The Taiwan military's IO-related strengths mainly include EW strengths and network warfare strengths, as well as PSYOP strengths.

(1) Electronic warfare strengths

The Taiwan military's EW strengths mainly are composed of professional-quality and nonprofessional-quality EW units of the three services, Army, Navy, and Air Force. The professional-quality EW units are the main force-strengths for implementing EW, and usually are employed per the principle of concentrated organizational grouping {*jizhong bianzu*} and unified application. They are mainly **[end of page 430]** responsible for EW attack missions such as electronic reconnaissance and detection {*dianzi zhence*}, electronic jamming, and electronic deception. As for the nonprofessional-quality EW units, their main mission is to conduct electronic counter-counter-suppression using existing electronic equipment, so as to protect the normal employment of friendly electronic equipment and systems.

1. Army EW strengths

The Taiwan Army General HQ's {*zongbu*} directly subordinate 72nd Communication Grouping {*tongxin qun*} is organized with 1 EW battalion; this battalion in peacetime has command over 1 EW company and 1 EW experimental company {*dianzihan shiyan lian*}, but in wartime is augmented by 3 companies. As the Army's only professional EW unit, it is directly managed and controlled by Army General HQ (Communication and Electronic Information Office {*tongxin dianzi zixun shu*}), and in wartime it respectively carries out electronic operations {*dianzi zuozhan*} missions for the various attached large formations (defending forces {*fangwei bu*}). Among these, the 6th, 8th, and 10th Large Formations each have 1 attached EW platoon.

2. Navy EW strengths

The Taiwan Navy is organized with 1 electronic operations group {*dianzi zuozhan dui*}, which is the Taiwan Navy's only professional EW unit. It is mainly equipped with 2 BJ-3 radar jammers {*leida ganraoji*}, which can conduct jamming against C-X-band [4.0-12.5 GHz] radar equipment, and have a maximum operating distance {*zuida zuoyong juli*} of 6-9 nautical miles {*haili*}; and has more than 2000 angular-type and circular-type reflectors {*jiaoxing, yuanxing fansheqi*}, which can reflect EM-wave signals and create false targets, to achieve the goal of imitation {伪冒 *weimao*}. The electronic operations group in peacetime participates in unit exercises and training {*yanxun*}, assists units at all levels in boosting their EW capability, assists in completing the setup {*sheding*} and updating {*gengxin*} of the ship automated EW system database {*jianting zidonghua dianzizhan xitong ziliaoku*}, and verifies {*yanzheng*} the EW response capability of Navy units. In wartime, based on the operational units' missions and needs, it adopts the mission organizational grouping mode {*renwu bianzu fangshi*} for the attached units to execute specific EW missions; or, based on operational-situation {*zhankuang*} needs and requirements, it will maneuver fishing vessels {*jidong yuchuan*} mounting circular-type and angular-type reflectors, to conduct electronic deception and [electronic] diversion/demonstration {*dianzi qipian he yangdong*}. In addition, Navy destroyers, escort gunships {*huhang paojian*}, and missile speedboats [fast attack craft]

{*daodan kuaiting*} are all outfitted with EW equipment {*dianzi duikang zhuangbei*} for electronic reconnaissance and detection, mechanical-style electronic attack {*jixieshi dianzi gongji*}, and radar protection. The Naval Aviation Command's {海军航指部 *haijun hang zhibu*} subordinate S-70C antisubmarine helicopters {*fanqian zhishengji*} also are equipped with ALR-606 electronic reconnaissance and detection systems. All of these have a certain EW capability. **[end of page 431]**

3. Air Force EW strengths

The Taiwan Air Force's EW strengths mainly are organizationally structured {*bianzhi*} within the Air Force's 20th EW Early Warning Air Group {*yujing dadui*}, under whose command are an early warning aircraft squadron, EW aircraft squadron, and communication counter-suppression detachment {*tongxin fanzhi fendui*}. These mainly are equipped with 4 E-2T and 2 E2-K AEW aircraft and 1 C-130HE electronic jamming aircraft, as well as with "Scorpio" {*"tianxiexing"*} ground-to-air communication jamming vehicles {*dikong tongxin ganrao che*}. Of these, the C-130HE electronic jamming aircraft's main missions are to conduct electronic attack and counter-suppression of reconnaissance and detection by the adversary's combat management system [CMS] {战管系统 *zhan guan xitong*} against friendly operational aircraft, so as to shorten the adversary's air defense early warning time, so that he cannot conduct effective interception {*lanjie*} of friendly main battle force-strengths, and to ensure the superiority of air defense operations. The communication counter-suppression detachment is equipped with 1 "Scorpio" ground-to-air communication jamming system, and mainly undertakes jamming missions against the adversary's ground-to-air communication. In addition, the Air Force's various models of main battle aircraft all are equipped with radar early warning and externally hung [pylon-type] and expendable electronic jamming equipment {*waigua, touzhishi dianzi ganrao shebei*}, which can provide directional and priority {*fangxiang ji youxian cixu*} early warning of the adversary's fire control radar {*huokong leida*}, and put into effect self-defensive electronic protection {*ziweixing dianzi fanghu*} via transmission of jamming waves or launch of expendable chaff or flame projectiles {*huoyan dan*}.

(2) Network warfare (CNO) strengths

Starting in 1998, the Taiwan military set about planning {*guihua*} establishment of network warfare units. After operations-research-based planning {*chouhua*} and preparations lasting up to 3 years, in January 2001 it formally established a "Communication and Information Command" {*"tongxin zixun zhihuibu"*}, to primarily undertake network warfare missions; and it planned {*guihua*} in Army, Navy, and Air Force units to further establish several professional network warfare detachments.

The Taiwan military's Communication and Information Command, besides undertaking tri-service communication duty assisting support and safeguarding support {*tongxin qinwu zhiyuan yu baozhang*} missions, also is responsible for executing network monitoring {*wangluo jiankong*}, defense {*fangwei*}, and counter-suppression

missions. As a professional network warfare unit, this command takes boosting of CNO {*wangluozhan zuozhan*} capability as the key point, and lists the safeguarding {*weihu*} of network security and the seizure of network warfare superiority as the main objectives to be pursued and developed. First of all, it exploits the superiority of the force-strengths deployed {*buyou*} at various spots on Taiwan, the Penghus [Pescadores], Kinmen [Quemoy], and Matsu {台, 澎, 金, 马 *tai, peng, jin, ma*}; prepares in various areas to establish organizationally grouped units with communication and information {通资 *tongzi*} network security missions; and is responsible for **[end of page 432]** security and reconnaissance and detection {*anquan zhence*} work for the armed forces' internal associated information networks, to ensure the normal operation {*yunxing*} of the Taiwan military's network systems.

The Taiwan military's professional network warfare detachments include the "Information Warfare Laboratory" {*"zixunzhan shiyanshi"*} set up under its "Ministry of Defense;" the "network attack teams" under the "IW Crisis Handling Centers;" and the various services' "critical emergency teams" {*"jinji yingbian xiaozu"*}, anti-virus combat situation centers {*fangbingdu zhanqing zhongxin*}, and anti-virus monitoring stations {防病毒监测站 *fangbingdu jiancezhan*}. Of these, the "IW Laboratory" is responsible for research and planning {*guihua*} for the advanced technology needed by the Taiwan military's network warfare; for designing, collecting, and storing {*chubei*} all types of computer virus programs {*bingdu chengxu*}; for maintaining {*weihu*} the "computer virus sample database" {*"diannao bingdu yangpin ziliaoku"*}; for designing and exploiting {*kaifa*} effective network warfare weapons; and for making preparations for wartime implementation of network attack and network system security protection. The network attack teams are mainly responsible for conducting monitoring {*jiankong*} of, and for finding loopholes and weak links in the mainland's military/civilian-use computer networks and web sites {*wangzhan*}, as well as in computer-controlled communication systems and wireless paging systems {*wuxian xunhu xitong*}, and in wartime conducting network virus attacks, to disrupt and paralyze important information systems. The "critical emergency teams" are responsible for monitoring and rapid response handling of all critical incidents, including reconnaissance and detection and counter-suppression of the adversary's network warfare attacks, and for strengthening the rapid repair capability for damaged systems {*shouchuang xitong*}. In addition, the Taiwan military also has established network warfare professional detachments in Army, Navy, and Air Force units. To give several examples, in the large formation and defending forces' communication battalions, it has further set up information platoons; the communication companies of the joint forces brigades {*lianbing lu*} have additionally organized information squads {*zixun ban*}; and all battalion communication platoons have additionally organized IO teams {*zixun zuoye zu*}. These are especially responsible for network management and erection, plus hardware maintenance {*yingjian weixiu*}, so as to form network warfare superiority.

(3) PSYOP strengths

The Taiwan military's PSYOP units mainly include political operations general elements {*zhengzhi zuozhan zongdui*} and Army PSYOP detachments {*xinzhan fendui*}. Of these, the political operations general elements are administratively subordinate to the General Political Operations Bureau {*zong zhengzhi zuozhan ju*}. They are the Taiwan military's professional units for executing PSYOP, literary and artistic propaganda {*wenyi xuanchuan*}, battleground agitation {*zhandi gudong*}, and government decree propaganda {*zhengling xuanchuan*}; and under their command are 3 groups {*dadui*} and 1 squadron {*zhongdui*}, viz.: a radio broadcast {*boyin*} group, a PSYOP {*xinzhan*} group, an artistic propaganda group, and a female youth {*nyu qingnian*} squadron. Of these, the radio broadcast group sets up "Han Sheng" {"汉声"} broadcast transceivers {*guangbo diantai*}, and in peacetime **[end of page 433]** is mainly responsible for conducting cultural propaganda for the Taiwan interior and for conducting PSYOP broadcasts against the mainland; and in wartime it is under orders {*fengming*} to undertake broadcasting operational missions. The PSYOP group is mainly responsible for missions such as network PSYOP {*wangluo xinli zuozhan*}, counter-PSYOP {*fanxinlizhan*}, air floats [i.e., giant balloons] {空漂 *kongpiao*}, and sea floats {海漂 *haipiao*}, and at the same time it is also responsible for assisting support to all operational units in implementing tactical PSYOP missions. The Taiwan Army's PSYOP detachments mainly include 1 PSYOP [company-size] detachment {*zhongdui*} and 1 PSYOP service [reorganization and outfitting] center {整备中心 *zhengbei zhongxin*} set up under the Army General HQ Political Department. The PSYOP [company-size] detachment in peacetime is only organized into 1 PSYOP contingent {*fenqiandui*} (tactical PSYOP detachment {*fendui*}), but in wartime, depending on the situation, it is augmented by a certain number of contingents, and mainly carries out tactical PSYOP missions. Under the PSYOP service center are set up a planning and guidance team {*jihua zhidao zu*}, an information and PSYOP team {*zixun xinzhan zu*}, and a logistics assisting support team {*houqin zhiyuan zu*}. In addition, the Kinmen [Quemoy] Defending Force also organizes 1 PSYOP work group {*xinzhan gongzuo zu*}. In order to boost its PSYOP capability, the Taiwan military also has built political operations schools {*xuexiao*}, used for cultivating (training) {*peiyang*} PSYOP professional talent.

III. Main activities of the Taiwan military's IO…434

The Taiwan military stresses that within information and electronic operations {资电作战 *zidian zuozhan*}, it should — based on the principle of a "combination of soft and hard attacks {*ruanying gongji*}, to ensure information and electronic superiority, and while conducting full-dimensional, multilevel, large-depth, uninterrupted reconnaissance and early warning — also achieve integrated application of tri-service advanced information and electronic operations weapons and equipment. Also via the dual tactics of "soft strike" and "hard destruction," it should suppress, harass-attack {*xirao*}, and disrupt the adversary information systems, and strive in the first strike to paralyze the adversary's C2 and intelligence information exchange {*qingzi jiaohuan*} capability, and weaken his tangible and intangible combat power.

(1) Electronic warfare

The Taiwan military holds that EW is an important counter-suppression means. It stresses that it should achieve integrated application of a variety of EW means, and place the key points on jamming and suppressing targets such as the adversary's search and tracking radar {*sousuo yu genzong leida*}, C2, communication, and weapons guidance systems, and information centers; degrading the effectiveness of the adversary's use of the EM spectrum; and thus seizing overall information and electronic superiority {*quanpan de zidian youshi*}. The Taiwan military's EW activities mainly include electronic offense and electronic protection.

Electronic offense mainly consists of stand-forward {前导式 *qiandaoshi*} electronic attack {*dianzi gongji*}, standoff {旁立式 *panglishi*} (long-range assisting support) electronic attack, escort {*bansuishi*} electronic attack, and self-defense {*ziweishi*} electronic attack. **[end of page 434]** The Taiwan military's attack search radar {*gongji sousuo leida*} generally uses standoff electronic attack, and applies high-power jamming equipment, outside the effective range (of fire) {*shecheng*} of the adversary's firearms {*huoqi*}, to carry out jamming and suppression of radar equipment. Its attack tracking radar {*gongji genzongshi leida*} generally uses stand-forward electronic attack, and dispositions {*bushu*} jamming units, unmanned aerial remotely-piloted vehicles [RPVs] {*wuren kongzhong yaokong zaiju*}, or prepositioned-route unmanned aerial vehicles [UAVs] {*yuzhi hanglu de wuren zaiju*} between the adversary's weapons systems and friendly operational units, to jam and suppress enemy radar equipment — or, it uses escort jamming {*bansuishi ganrao*}, and applies strengths or equipment to execute the electronic attack, and accompany the operational units' activities, to jam and suppress the adversary's radar equipment. When [conducting] operations within the adversary's weapons range, it mainly uses escort jamming as primary.

The Taiwan military divides electronic protection into two large types: counter-electronic reconnaissance and detection {*fandianzi zhence*} and counter-electronic attack {*fandianzi gongji*}. The basic tactics {*zhanshu*} for its electronic protection include the following: it applies local or all-around EM-wave emission control {*fashe guanzhi*}, and strengthens the intelligence transmission and security techniques {*qingbao chuanshu yu baomi jishu*}, to protect friendly emitted EM waves from the adversary's reconnaissance and detection, exploitation, and attack; and it adopts a variety of techniques and measures to strengthen the electronic defense capability and readiness {*zhanbei*} measures for friendly C2 systems and weapons and equipment, to increase the adversary's degree of difficulty in electronic attack, and to ensure that the friendly side can effectively employ the EM spectrum and bring into play the effectiveness of informationized equipment.

(2) Network warfare

This includes network intrusion and guarding against intrusion {*fangzhi ruqin*}. The Taiwan military requires that its network warfare strengths should fully apply network attack equipment to execute full-dimensional network attacks against the

adversary's various types of information, information flow, information systems and equipment, and information infrastructure, so as to paralyze the adversary's command systems and degrade his operational capability. Having conducted research over many years, the Taiwan military has already realized certain achievements in the research respects of network attack means, such as computer viruses and computer [EM] pulse bombs {*diannao maichong zhadan*}. Its main fighting methods {*zhanfa*} include the following several types: first is concealed intrusion {*yinbi ruqin*}. This is the use of reconnaissance modes such as network scanning {*wangluo saomiao*} to seek {*xunzhao*} back-door loopholes {*anmen loudong*} within the adversary's computer networks, and in concealed, hacking form {*feifa de xingshi*} enter the adversary's computer and network systems. The second is direct intrusion {*zhengmian ruqin*}. This indicates entering a secret code {*jinru mima*} which breaches {*pojie*} the target computer or network system, **[end of page 435]** or using a valid identity {*hefa shenfen*} to enter the adversary's computer or network system. Third is masking intrusion {*weizhuang ruqin*}. This means sneaking into {*hunru*} the internal network address {*neibu wangzhi*} masked within the target network system, to conduct hacking activity {*feifa huodong*}. Fourth is deception intrusion {*qipian ruqin*}. This means posing as {*maochong*} a network system manager, exploiting modes such as sending of e-mail or calling up a computer user to require him/her to provide a secret code [i.e., password] to facilitate carrying out system maintenance {*weihu*}, and then using the swindled code [password] to enter the adversary's computer network system. Fifth is virus intrusion {*bingdu ruqin*}. This indicates exploiting a virus preinstalled {*yushe*} within the computer, to have specific data/resources {*teding ziliao*} within the adversary computer transmitted back to one's own computer. Sixth is spam intrusion {*laji ruqin*}. This means sending large quantities of spam {*laji xinxi*} to the target computer or network, and causing its system due to overloading {*fuhe guozhong*} to produce mistakes or freeze up {死机 *siji*}.

The Taiwan military's informationized degree {*xinxihua chengdu*} is fairly high. It attaches unusual importance to guarding against intrusions, and in regard to defending against the adversary's intrusions into its critical computer networks or military systems, the Taiwan military often exploits network firewalls {*wangluo fanghuoqiang*}, separates {*gekai*} the hosts {*zhuji*} for internal networks from the hosts which provide external services {*duiwai fuwu*}, and filters unknown network actions {*xingwei*} and resources/data {*ziliao*}, so that even if computer hackers intrude into the server host, they still will not be able to penetrate the server host and enter the internal network system. Within the process of computer network operation {*yunxing*}, the Taiwan military strictly adopts measures such as electronic-cipher authentication cards {*dianzi mima renzheng ka*}, fingerprints, and facial recognition {*rongmao bianshi*}; and when entering network operations {*wangluo zuoye*}, everyone establishes a pass code {*tongxing ma*}, and regularly changes it. The Taiwan military also adopts methods such as network infiltration security checks {*wangluo shentou anquan jicha*}, network-intrusion real time identification and response, network access monitoring/control and management inspections {*wangluo cunqu jiankong yu guanli jicha*}, and e-mail defense and inspections, to strengthen the management of important networks.

(3) PSYOP

The Taiwan military holds that traditional PSYOP takes attacks on popular feeling {*renxin*} as the operational objective, while the various types of information activities within modern war — CNO, intelligence warfare, and EW — also all attack the adversary's psychology. Hence, the means of PSYOP also are the means of IW {*zixunzhan*}, and the objectives of PSYOP also are the objectives of IW. The Taiwan military holds that future operations first of all must rely on intensive {*miji*}, high-efficiency, real-time information collection systems, **[end of page 436]** to gain superiority in intelligence respects, so as to create good conditions for information deterrence {*xinxi weishe*}. After that, via intense information suppression to interdict {*zheduan*} the operational opponent's information propagation avenues, or by exploiting satellite direct broadcasts {*weixing zhibo*} and other modern media tools to conduct propaganda on the might {*weili*} of high/new-tech weapons {*gaoxin wuqi*}, one broadcasts untrue information {*bushi xinxi*}, to exert pressure on him. Finally, by displaying the operational intention, one shakes the opponent's psychology, causing him to lose confidence and his defensive line {*fangxian*} to collapse, so that he loses the will to resist and the capability to deal with crises.

Before combat or during combat, the Taiwan military also intends — via modes such as developing network PSYOP, controlling {*guanzhi*} and applying the media, enhancing popular support and morale {*minxin shiqi*}, strengthening education for the officers and men {*guanbing*}, and guarding against network intrusions — to strengthen psychological protection, and boost PSYOP protection capability.

(4) MILDEC

The Taiwan military holds that MILDEC and PSYOP both belong to stratagem-quality actions {*mouluexing zuowei*}. It requires that MILDEC should be closely complemented {*miqie peihe*} by means such as network warfare, EW, fire strikes, and modern media, and be mutually adjusted-coordinated with other operational activities, to deter the adversary, confuse what is seen and heard {*shiting*}, and cause assessments without grounds and decision-making errors.

The activities of the Taiwan military's MILDEC are diverse. The common ones are as follows: employing computer networks to transmit false information to the adversary, exploiting broadcast networks {*guangbo wangluo*} to conduct propaganda with false messages, and exploiting mobile radar {*jidong leida*} and instruments {*yiqi*} which can transmit same-power signals in different locations to transmit signals, create false impressions {假象 *jiaxiang*}, and interfere with the adversary's assessments and decision-making; setting up {*shezhi*} false targets, or exploiting vegetation {*zhibei*}, natural protective screens, and advanced technical means, to carry out camouflage and defilading {*weizhuang, zhebi*} of important targets; applying airborne launchers {*jizai fasheqi*} to project metal chaff {*jinshu ganraosi*} and flame projectiles to jam and

deceive the adversary's reconnaissance systems; and adopting various deception techniques to confuse the opponent and to complement the main operational activities.

(5) Entity attacks {*shiti gongji*}

The Taiwan military holds that the hard strikes executed by applying special operations forces {*tezhan budui*}, precision guided munitions [PGMs] {*jingque zhidao wuqi*}, anti-radiation weapons, and directed energy weapons [DEWs] {*zhixiangxing nengliang wuqi*} against the adversary's various information and electronic systems and equipment installations — air defense radar, communication hubs {*tongxin shuniu*}, electric power system nodes, radio and TV stations, etc. — are called entity attacks, and are important means for information and electronic operations. In wartime, one should, based on information and electronic operations **[end of page 437]** integrated-whole planning {*zhengti jihua*}, tightly center on the main operational activities of joint operations, and rationally apply entity attack strengths, mutually complemented by various soft means of information and electronic attack, to seize battlefield information and electronic superiority.

IV. IO capabilities of the Taiwan military…438

Although the organizational structure of the Taiwan military's IO units is not large, nonetheless its means are complete. It possesses various types of anti-aircraft {*duiji*} (including C-130HE EW aircraft), anti-ship {*duijian*}, and anti-submarine {*duiqian*} electronic jamming and counter-jamming equipment. A good many pieces of the Taiwan military's IO equipment belong to the same standard {制式 *zhishi*} as the US military's active-duty electronic equipment, and the performance of its main IO equipment has almost reached the same level as that of the US military, so it has a fairly strong IO capability.

(1) Electronic warfare capabilities

1. Electronic reconnaissance capabilities

Electronic reconnaissance is under the unified adjusting-coordination and control {*guanzhi*} of the Military Staff HQ {*canmou benbu*} Telecommunications Development Section {电讯发展室 *dianxun fazhan shi*}. It mainly employs ground electronic reconnaissance stations and electronic reconnaissance aircraft, as well as electronic reconnaissance equipment carried on operational ships, to conduct strategic and tactical electronic reconnaissance against the adversary.

(i) Ground electronic reconnaissance capability

At present, the Taiwan military mainly uses electronic reconnaissance stations on Taiwan Island and the peripheral islands, to intercept and detect the mainland's various

types of message ELINT {信电子情报 *xindianzi qingbao*}. Among these, the Military Staff HQ's Telecom Development Section has set up several electronic reconnaissance stations on Taiwan Island, and has set up work teams {*gongzuo dui*} on Kinmen [Quemoy], Matsu, and Dongyin [at the northeast tip of the Matsu group]; its Military Intelligence Bureau has set up electronic reconnaissance stations (teams) on the outer islands; and its Army Technical Research Division {*lujun jishu yanjiu chu*} has set up electronic position-finding stations {*dianzi ceweizhan*} at Chang-hua and Tai-nan [in central and southern Taiwan, respectively]. These electronic reconnaissance units {*danwei*} in peacetime uninterruptedly conduct radio reconnaissance of the adversary, and are capable of fairly effectively detecting the adversary's radio signals in the southeast seacoast area and in the Taiwan Strait, and of conducting analysis and arrangement and storage {*zhengli chucun*} of the adversary's ELINT it has collected, so as to carry out electronic jamming and electronic counter-jamming against the adversary. **[end of page 438]**

(ii) Air electronic reconnaissance capability

The [Taiwan military's] air electronic reconnaissance mainly is conducted by electronic reconnaissance and early warning aircraft fielded by the Air Force EW squadrons and AEW aircraft squadrons, and by the Air Force's ground ELINT stations. At present, the Air Force uses AT-3 model EW and C-130HE EW aircraft to conduct surface-to-air reconnaissance {*duikong zhencha*}. These can capture our side's radio/wireless communication and radar signals, and on such grounds analyze and assess the disposition and traits {*texing*} of our side's radio/wireless communication, the coverage scope of [our] radar systems, and [our] deployment gaps {*peizhi jianxi*} and observation blind areas {*guance mangqu*}. The electronic reconnaissance and detection systems of the E-2T model early warning aircraft are outfitted with fairly high-function signal and data processors {*xinhao, shuju chuliji*} and databases. These can rapidly intercept signals, classify {*fenxuan*} signals, and identify targets, and can detect/measure {*zhence*} the signal parameters of the electronic radiation sources, including radar and IFF devices {*diwo shibieqi*}, with which our air, ground, and sea weapons systems are equipped.

In addition, the Air Force Electronic Monitoring Center {电子监察中心 *dianzi jiancha zhongxin*} also uses its subordinate monitoring detachments {*jiancha fendui*}, electronic direction-finding stations, and electronic reconnaissance stations (teams) to collect radio signals and conduct reconnaissance and detection of our Air Force's communication networks and communication situation in the southeast seacoast area.

(iii) Sea electronic reconnaissance capability

The American-made SLQ-32(V)2 EW systems installed on the [Taiwan] Navy's *Knox*-class missile frigates {*daodan huweijian*} and the "Chang Feng 4" {"长风4号"} EW systems installed on the *Cheng Kung*-class missile frigates all have very strong electronic reconnaissance capability; they can effectively detect our side's radar and

communication signals, and automatically carry out signal classification and identification {*xinhao fenxuan, shibie*}. In addition, the combat intelligence elements {*zhandou qingbao dui*}, direction-finding stations, and technical reconnaissance teams {*xiaozu*} subordinate to the Navy Communications Research Section {*tongxin yanjiushi*} can fairly effectively monitor {*jiankong*} radio/wireless communication between our naval ships in the Taiwan Strait area and their bases.

2. Electronic jamming capability

[The Taiwan military's] electronic jamming operations mainly consist of the professional strengths of the Army communication and EW groupings {*tongxin dianzizhan qun*}, the EW companies of all large formations, the Penghu Defending Force's EW platoons, and the Air Force's EW squadrons and AEW aircraft **[end of page 439]** squadrons. These conduct suppressive and deceptive jamming.

(i) Ground jamming capability

At present, the [Taiwan] Army EW units are equipped with US-produced and Taiwan self-made {*zizhi*} multiple types of communication jammers and radar jammers. Of these, the communication jammers can carry out jamming of our side's shortwave and USW AM and FM communication; and the radar jammers can carry out jamming of the adversary's battlefield surveillance radar and target detection radar {*mubiao zhence leida*}. The Taiwan joint forces brigades {*lianbing lu*} in wartime can obtain the reinforcement {*jiaqiang*} of two electronics companies, which are equipped with 9 sets of electronic equipment. Their ground communication interception range is 20 km, air interception range can reach 100 km, ground communication jamming range can reach 30 km, and air communication jamming range can reach 40 km. This equipment can simultaneously suppress a number of HF/VHF {*gaopin/shengaopin*} communication dedicated networks {专网 *zhuanwang*} of the adversary. If they can obtain air and ground electronic support {*dianzi zhiyuan*} [ESM] from higher levels or from a powerful nation {*qiangguo*}, their electronic offense capability can simultaneously suppress 34 dedicated networks.

(ii) Air jamming capability

The Taiwan Air Force attaches extreme importance to the development of self-defense EW capability for its aircraft. Besides the imported 1:1 full complement {*peitao*} of self-defense EW equipment (systems) on the F-16s and Mirage 2000s, it also has imported from Israel and other nations self-defense electronic jamming equipment such as electronic jamming pods, radar warning devices {*leida gaojingqi*}, and chaff/IR dispensers {*botiao/hongwai toufangqi*}, and supplied them for use in refitting {*gaizhuang*} its active-duty aircraft. Almost all of its active-duty aircraft have self-defense EW equipment. The F-16 models are equipped with AN/ALQ-184 electronic jamming pods, which can automatically identify threat signals {*weixie xinhao*}, and, based on the nature of the threat, select the optimal jamming mode, jamming direction,

and jamming beam {*ganrao boshu*}, to conduct effective electronic jamming against the target aircraft and missiles. The above jamming equipment, when conducting jamming against various models of ground radar, as well as radio/wireless communication network platforms {*wangtai*}, have an effective operating distance {*zuoyong juli*} of as much as 100 km or more. If the jammers fly along the Taiwan Strait center line, they can produce quite strong jamming of most radar [sets] in the southeast seacoast area. **[end of page 440]**

(iii) Sea jamming capability

[Taiwan's] naval electronic operations missions mainly are undertaken by Navy surface operational ships {*shuimian zuozhan jianting*}. At present, its destroyers, frigates, and missile speedboats [fast attack craft] are mostly outfitted with fairly advanced EW equipment {*dianzi duikang shebei*}, and staffed by special-duty {专职 *zhuanzhi*} [i.e., "specialist"] EW {*dianzizhan*} personnel. The ultrahigh-speed hull-mounted dispersed passive jamming chaff and IR decoy launch system {*chaogaosu jianwai sankai wuyuan ganrao botiao he hongwai youer fashe xitong*} installed on the *Knox*-class ships is integrated {*yiti*} with the ship-mounted electronic reconnaissance system, IR warning system, and fire control system; and under computer control, according to a program {*chengxu*}, it automatically launches chaff projectiles {*botiao dan*} and IR decoy missiles {*youer dan*}, with a maximum range (of fire) of 2000m, and a single-shot chaff projectile RCS which can reach 4000 square meters. The *La Fayette*-class [ROC *Kang Ding*-class] frigates are equipped with new-generation simulated EW systems {*monihua dianzizhan xitong*} and "Dagaie" {"达盖"} passive chaff launch device, which give them fairly strong electronic suppression, counter-suppression, and threat warning capabilities. The *Perry*-class missile frigates are equipped with AN/SLQ-32 integrated EW systems, as well as with the MK-36 model passive jamming chaff and IR decoy launch system. The AN/SLQ-32 integrated EW system's main function is to carry out detection {*tance*}, identification, direction-finding, and alarm issuing for approaching radar-guided anti-ship missiles {*leida zhidao fanjian daodan*}; but at the same time, this system can control the shipborne MK-36 passive jamming chaff and IR decoy launch system. In addition, the shipborne jamming rockets {*jianyong ganrao huojian*} developed by the Taiwan Academia Sinica [Academy of Sciences] {*zhong ke yuan*} can be installed with electronic jamming smoke bombs {*dianzi ganrao yanwudan*}; at range of 2000m, these form a jamming screen {*ganraomu*} and create false targets, causing incoming missiles to deviate from course, and effectively counter-suppressing missiles of different guidance systems.

3. Electronic defense capability

(i) Radar early warning system electronic protection capability

Today, the Taiwan Military Staff HQ's "Heng Shan," the Air Force's 'Ch'iang Wang," the Navy's "Ta Ch'eng," and the Army's "Lu Tzu" command automation systems {*zidonghua zhihui xitong*} already have respectively realized computer

networking {*jisuanji lianwang*}. They can carry out unified control {*tongyi guanzhi*} of intelligence acquired by the Air Force's various control and reporting stations {*guanzhi baogao zhan*} and the Navy's various radar observation and communication stations {*leida guantong zhan*} plus its airborne and shipborne radar, and have enabled their radar early warning systems **[end of page 441]** to form a wideband {*kuanpindai*} radar signal spatial net {*leida xinhao kongjian wang*} with a fairly high signal concentration {*xinhao mijidu*}. All radar [sets] are mutually coordinated {*xianghu xietong*} and mutually alternating {*xianghu jiaoti*}, which has boosted integrated-whole jam-resistance capability {*zhengti kangganrao nengli*}. In the newly fielded E-2T model early warning aircraft, the radar jammers have a peak power as high as the megawatt [MW] level {*zhaowa ji*}, and adopt pulse compression {*maichong yasuo*} technology; they have pulse frequency agility {*maichong pinlyu jiebian*} and pulse-group frequency agility {*maizu pinlyu jiebian*} capability, and thus are not easily jammed.

(ii) Communication system electronic protection capability

The Taiwan military's ring-island fiberoptic cable net {*huandao de guanglan wang*}, and its seabed fiberoptic cable net linking Taiwan to the outer islands, including Kinmen, Matsu, and Wuchiu [Wuciou, west of Hsin-chu in the Taiwan Strait], have already been completed, added to which is the building of a number of satellite receiving stations. The [military's] communication system already has basically activated a 3-D communication net {*liti tongxin wang*} composed of underground (seabed) cables (fiberoptic cables), ground microwave {*dimian weibo*} [relays], and outer space communication satellites {*taikong tongxin weixing*}. These networks can automatically switch over among one another, and have provided a jam-resistance capability for this communication system.

(2) Network warfare capability

In computer information network warfare [CNO] {*jisuanji xinxi wangluozhan*} respects, the Taiwan military already has the capability to attack our civilian information networks, and has now set about implementing its "computer network information warfare" {*"diannao wangluo zixunzhan"*} plan. The Taiwan "Ministry of Defense" has already organized a standing computer hacker team {*changbei heike xiaozu*} specializing in reconnaissance and detection {*zhence*} and recording of loopholes in mainland web sites {*wangzhan*} and their patch {*xiubu*} situation as a technical reserve {*chubei*} in wartime. At the same time, it has newly organized research teams {*yanjiu xiaozu*}, and lays stress on studying the security {*anquanxing*} and attackable quality {*kegongjixing*} of mainland telecom IP [Internet Protocol] telephone networks. Exploiting the mainland's reliance on Taiwan-made computer accessories {*jisuanji peijian*}, it plans to embed virus chips {*qianru bingdu xinpian*} within products sold to the mainland, and under suitable conditions, via remote-control triggering {*yaokong chufa*} of the viruses, thus disrupt [sabotage] {*pohuai*} computer systems and user data. Once shooting begins in a war, Taiwan will add in certain special signals {*teshu de xinhao*} within the electronic jamming signals it transmits. The hardware of all computers within the operating range

{*zuoyong fanwei*} of this electronic signal may then respond on the computer bus {*jisuanji zongxian*} to the weak jamming trigger signal {*weiruo de ganrao chufa xinhao*}, thus triggering the virus.

Purely in software respects, [Taiwan] by and large has partitioned its targeting {*zhendui*} of the mainland's prevalent operating systems {*caozuo xitong*} in three respects: the first is the "D&W Darwin Plan {达尔文计划 *daerwen jihua*}, where the targets of attack {*gongji duixiang*} are **[end of page 442]** machines running the DOS and Windows [D&W] operating systems; and the associated hardware's full set of drivers {*peitao de qudong chengxu*} are one of the main propagation avenues. Second is the "Jasmine Plan {*moli jihua*}," targeting Linux and UNIX, as well as the VAX/VMS system relatively prevalent within the mainland's scientific research units {*keyan danwei*} and education departments. Third is the highly secret {*baomi*} Internet network plan. One Taiwan network research team already has resolved the network trigger and control problems for computer viruses.

(3) PSYOP capabilities

The Taiwan military holds that war also is a struggle of will between the two sides, and that strength or weakness of spirit {*jingshen*} is the key in deciding victory or defeat in war. However, spirit is produced by psychology; thus, psychological warfare is especially important compared to operations with tangible weapons.

What the Taiwan military currently adopts is a peacetime-wartime combined {*pingzhan jiehe*} PSYOP defensive SoS {心防体系 *xinfang tixi*}. Taiwan's "Ministry of Defense" has established lieutenant colonel/commander [rank] {*zhongxiao*} psychological guidance officers {心理辅导官 *xinli fudao guan*}, responsible for policy research and formulation {*zhengce yanding*} for armed forces-wide psychological health work {*quanjun xinli weisheng gongzuo*} and for executing supervising-guiding {*dudao*}; the general HQs {*zongbu*} of all services have established major/lieutenant commander [rank] {*shaoxiao*} psychological guidance officers, who supervise-guide all division-level and higher units (including the joint-forces brigades and all military colleges and schools {*yuanxiao*}) in establishing "psychological health centers," and regularly conduct psychological health (guidance) lectures and studies {*jiangxi*} and circuit education {*xunhui jiaoyu*}; and the large formation, corps, and joint-forces brigade units have established captain/lieutenant [rank] {*shangwei*} psychological guidance officers. All services' general HQs and military police command HQs {宪令部 *xian lingbu*} watch the situation to guide and plan {*guihua*} the dispatch {*diaopai*} of officers, NCOs, and men {*guan, shi, bing*} or hired personnel having professional knowledge {*zhuanye zhishi*} as well as zeal for service {*fuwu rechen*}, to assume the post of assistant guidance teacher {*zhuli fudao laoshi*}. The Taiwan military specifies that all levels of political warfare departments {政战部门 *zhengzhan bumen*} and political warfare officers {政战军官 *zhengzhan junguan*} have full authority {*quanquan*} for psychological guidance activity in the responsible departments. Company guidance heads {连辅导长 *lian fudao*

zhang} hold concurrent posts {*jianren*} as 1st-line "psychological guidance officers" {"心辅官" *"xin fu guan"*}, responsible for taking initiative to grasp those officers and men whose morale is unstable {*qingxu buwen*}, and assist them in unhurriedly resolving {舒解 *shujie*} psychological problems. Psychological guidance officers at the "psychological health centers" handle cases turned over after company-level guidance {*liandui fudao*} has failed to show significant improvement; and "area {*diqu*} psychological health centers" then combine hospital treatment resources with social support {*zhichi*} networks, to carry out concentrated guidance, and bring into play the reconstructive functions {*chongjian gongneng*} of corrective treatment {矫治 *jiaozhi*}, medical treatment, and psychology.

In order to defend against the adversary's psychological offensives {*xinli gongshi*} and strengthen control over the thought behavior {*sixiang xingwei*} of the officers and men, the Taiwan military attaches extreme importance to the establishment and improvement of a PSYOP defensive SoS {*xinzhan fangyu tixi*}, and in particular, the Taiwan military's psychological guidance activity has become the center of attention {引入注目 *yinru zhumu*}. Starting in 1990, it set up "psychological health centers" within the corps, **[end of page 443]** on the "Ministry of Defense Global Information Network {*quanqiu zixun wang*}" it set up psychological guidance web sites {*xinli fudao wangzhan*}, and within the units it universally established a psychological guidance system {*xin fu zhidu*}. The aim is to announce, guide, and popularize {宣导推广 *xuandao tuiguang*} psychological health education, and rely on professional psychological consultants employing the consultation and interview mode {*zixun wutan fangshi*}, to rectify {导正 *daozheng*} officers and men [showing] deviant psychology and behavior, and mutually complement {*xiangfu xiangcheng*} this with management and instructional {管教 *guanjiao*} measures, to properly adjust {调适 *tiaoshi*} their psychology, improve their character {*renge*}, and eliminate problems hiding in the officers and men, [to achieve] solid unit combat power {*jianshi budui zhanli*}. **[end of page 444; end of book]**