AIR WAR COLLEGE

AIR UNIVERSITY

THE END OF HEGEMONY:

TECHNOLOGIES OF A NEW TRIPOLAR WORLD

By

Paul R. Fiorenza, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2012

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instructions 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lt Col Paul Fiorenza is a US Air Force pilot assigned to the Air War College, Air University, Maxwell AFB AL. He graduated from the Clarkson University, Potsdam NY in 1992 with a Bachelor of Science degree in Computer Engineering and from the University of Tennessee in 2009 with a Master of Science degree in Aviation Systems, concentration in Flight Test. He earned his pilot wings in 1994, graduated from Navy Test Pilot School in 2003, and completed seven combat deployments to CENTCOM as a Combat Search and Rescue pilot and an Iraqi Air Force Aviation Advisor. He has over 2200 hours flying more than 20 types of military fixed wing and rotary wing aircraft, with primary qualifications in the HH-60G, MI-17, UH-60A, OH-6, C-12, and UH-1N. He has commanded a geographically separated flight test detachment and has served on the Air Staff in Acquisitions and Congressional Liaison positions.

Abstract

The era of US global hegemony is drawing to a close. Within the next quarter century, revolutionary technological developments and new military capabilities will fracture the geopolitical strategic landscape, propelling today's near peer states into a parity position with the US. A shift to an information-centric globe will see ongoing conflict over the control of information through the new global commons of space and cyberspace. Technological advances in these areas coupled with the deterrent value of nuclear weapons will reduce the effectiveness of US conventional forces, and US interests will be challenged on a global scale. A new reality of continuous conflict over information will emerge in space and cyberspace where it will not be possible for a single state to maintain dominance. Through a deliberate focus on information and space control technologies, China and Russia are positioned to gain strategic military parity with the United States, resulting in the emergence of a new tri-polar world.

Three examples of technologies critical to the conflict over information control are explored: information warfare, space operations, and nuclear weapons. The Chinese have embarked on a campaign of "Informationization" to attain mastery of both the electromagnetic spectrum and the global cyber sphere. This approach includes the attempted dominance of air, space, and cyber mediums, through cyber operations, information operations, electronic attack, and kinetic attack. Given the Chinese view that there are no distinct boundaries between peacetime and wartime information warfare, the Chinese should be expected to employ this capability across the spectrum of conflict.

China is also preparing for an "inevitable" competition in space, as it is recognizes that "controlling space controls the globe." Chinese authors have discussed multiple space attack

methods to include kinetic attack, directed energy attack, electronic attack, and ground attack of satellite control signals and control stations.

The third technology example illustrates the Russian Federation's robust research, and development program focused on an entirely new class of "fourth generation" nuclear weapons. This new weapons technology will introduce exquisite low yield weapons within the next 20 years. These weapons combined with a Russian theory of "de-escalation" through the limited use of nuclear weapons points to a more aggressive posture than the one signaled in Russia's written doctrine.

We are in the midst of a shift in strategic eras from the traditional American way of war through mass and dominance to an ambiguous state of constant conflict over information. In this new era, the effectiveness of today's conventional global strike will be reduced to the point where it is of limited deterrence value. Due to their significant infrastructure, matched with a doctrinal emphasis on aggressive use of space, cyberspace, and nuclear weapons, the threat of conflict over control of information with China and Russia should not be taken lightly. The US must recognize that it will not be able to control the new domains of cyber and space as it has enjoyed the control of the sea and air, and must appropriately prepare for this new reality.

Table of Contents

Introduction

The era of US global hegemony is drawing to a close. Within the next quarter century, revolutionary technological developments and new military capabilities will fracture the geopolitical strategic landscape, propelling today's near peer states into a parity position with the US. While a flattening world promises to bring new capabilities to all nations and even individuals, nation states that are able to support long term, focused, and well funded research and development programs are uniquely poised to capitalize on emerging technologies for military gain. Through a deliberate focus on information and space control technologies, China and Russia are positioned to gain strategic military parity with the United States, resulting in the emergence of a new tri-polar world.

A shift to an information-centric globe will see ongoing conflict over the control of information through the new global commons of space and cyberspace. Technological advances in these areas coupled with the deterrent value of nuclear weapons will reduce the effectiveness of conventional forces enabling China and Russia to challenge US interests on a global scale. A new reality of continuous conflict over information will emerge in space and cyberspace where it will not be possible for a single state to maintain dominance to the degree that the US has over the last 60 years. States operating in these new unexplored, and even undefined global commons will, at best, control narrow slices of space and cyberspace for limited periods of time.

The future of warfare is on the precipice of radical change. In their 1993 book "War and Anti War", Alvin and Heidi Toffler posit that "the way we make war reflects the way we make wealth".[1] Following the economic transformation of the Industrial Revolution, warfare in the 19th and 20th centuries transitioned to one based on industrial capacity. As the 21st century world transitions to a post industrial-economy, more and more global wealth will be generated through

the flow of information. The term "information economy" was popularized in a 1967 study that found 53% of the US economy was engaged in knowledge work. By 1997 it was calculated that 64% of the US economy was based on information. [2] While current estimates vary, today's information economy has certainly grown to the point where almost all forms of trade are integrated into the information economy through commerce, communications, and banking. Warfare will correspondingly shift to a conflict over the control of this information.

The nature of the rising conflict over information in the new global commons of space and cyberspace are far different from the mediums that the US currently operates in with nearly unchecked freedom of action. Due to the attributes of the new global commons of space and cyberspace, this level of dominance will be lost. Space and cyberspace will be an ambiguous environment marked by speed of light actions and challenging attribution resulting in a continuous, modulated level of conflict with the potential for rapid escalation. This new reality will lead to an inevitable state of parity between the US, China, and Russia, driving a state of constant conflict in the struggle over space and cyberspace control.

Of course, the role of conventional forces will not diminish entirely. Robust land, naval, and air forces will be necessary to control territorial borders and maintain regional stability. Due to the growth of anti-access/area denial capabilities over the next decade, however, the ability for conventional forces to project power globally will be significantly reduced.[3] This reduction in effectiveness will be further reduced by increases in intelligence, surveillance, and reconnaissance capabilities of large nation states by leveraging information through space and cyberspace. The conflict over information will arise as the precise location, operating procedures, and even computer algorithms of an adversary's conventional forces become known. The nation that can best control the information environment will have vast strategic advantage. In this way, it may be possible for near-peer states to gain coercive leverage over the US without

matching US investment in expensive conventional ground, naval, and air forces. When this happens the effectiveness of conventional deterrence through threat of a kinetic strike will be significantly diminished.

This shift to an information-centric globe will have profound effects on the military strategy. The strategic ends, ways, and means of nation states will shift to become more focused on the control of information. In this world, information control will be the strategic ends achieved through the control of space and cyberspace (the ways), enabled by a nation's educated human capital able to operate in these mediums. As the transition occurs to a conflict over the control of information it will still be necessary to deter territorial aggression against the homeland. While conventional forces will have reduced importance, nuclear forces will provide deterrent from territorial aggression. Along with the United States, China and Russia are uniquely poised to succeed in a struggle over control of information due to their robust capabilities, infrastructure, and funding available to develop technologies in the cyberspace, space, and nuclear technology areas.

Three examples of the technology areas critical to the conflict over information control are explored in this paper: Chinese information warfare concepts and technologies, Chinese space operations, and Russian nuclear weapons development. These technology areas should not be viewed in a vacuum, as it is the combination of all three that will provide national power during the transition to an information-centric strategic era. Furthermore, these are simply examples of the approach that is being taken. Both China and Russia have robust capabilities in all three areas and have the infrastructure, funding, and human capital to leverage these areas in the future. Additionally, to better understand the application of these technologies, this paper

evaluates Russian and Chinese doctrine to help assess how the technology might be used in a future conflict.

---

[1] Alvin Toffler and Heidi Toffler. *War and Anti War.* Boston: Little, Brown, and Company, 1993, 4.

[2] Apte, Uday, and Hiranya Nath. "Size, Structure and Growth of the US Information Technology." January 2004, http://www.anderson.ucla.edu/documents/areas/ctr/bit/ApteNath.pdf, *i.*

[3] The Center for Strategic and Budgetary Assessments has studied the impact that the Chinese anti-access / area-denial strategy will have on US interests. In an interview with Jim Thomas, he recently asked the question "Is this the post-power-projection era?" as quoted in Manea, *Interview with Jim Thomas.*

China and Russia: Capability, Intent, and Opportunity

While military capability is the focus of much of this paper, to truly evaluate the potential threat of a nation state to US interests, intent and opportunity should be part of the overall calculus. In the case of China, James Clapper, Director of National Intelligence testified to the House Permanent Select Committee on Intelligence on February 10, 2011 that "China's external behavior remains inextricably linked to the leadership's overarching concern with maintaining economic growth and domestic stability."[4] Changes in domestic context have the possibility of rapidly adjusting a nation's military intent with respect to other nations. Therefore, a top level discussion of national issues is necessary in order to better understand China and Russia's approach to leveraging new weapons and capabilities likely to emerge by 2035.

China

Today, China sees a parallel between the Warring States period of the 3rd and 4th centuries BC and today's geopolitical framework, with the world moving toward multi-polarity. China foresees a world dominated by US, China, Russia and Japan, where India and Germany play important but lesser roles in geopolitics.[5] Within this context China continues to be guided by Den Xiaoping's "24 Character" strategy, translated as "Observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership."[6] Publicly, China sticks to this strategy. During a visit to the US in January 2011, Chinese President Hu Jintao, stated "We do not engage in an arms race. We are not a military threat to any country."[7] Given the rise of Chinese national power over the last 20 years, however, there is currently a conflict between a desire for more international deference and the desire to maintain its peaceful rise during a "window of strategic opportunity."[8]

Within the first decade of this century, the rise of China appears to have been accelerated through aggressive economic development and parallel financial challenges of the US. Along with China's economic rise, its military capabilities have changed dramatically in the last two decades. Following the 1991 Gulf War, China began an ambitious program to modernize its military and has made significant strides in high technology weapons sets. The Department of Defense's estimate of China's military related spending in 2009 was $150 billion.[9,10] During 2008 and 2009 China's military spending increased 17.5% and 18.5% respectively before moderating to 7.5% in 2010.[11] Given the looming cuts to US defense budgets coupled with a conservative outlook of 5% to 10% annual growth rate of China's economy, it can be seen that the two trend lines of declining US defense spending and increasing Chinese defense spending will soon cross. From a market rate view point this is expected to occur in the early 2020s, however, when adjusted for purchasing power parity the lines will cross much sooner.[12]

While China publicly discusses a peaceful rise, it is investing significant resources in advanced technology weapons, sending a conflicting signal to the rest of the world. China sees the first twenty years of the 21st century as a "period of opportunity" for a peaceful increase in military capability[13], however, what looms after this timeline is less clear. Writings in Chinese military journals point to significant investments in "magic weapon trump cards", or advanced technology weapons that have the possibility of overcoming an adversary through asymmetric means. For example, China is pursuing counter-space and cyber capabilities that threaten space and cyber based information infrastructure.[14] China put the world on notice that it had a robust counter space program with its successful demonstration of a direct-ascent antisatellite weapon in January 2007. [15]

There is a significant contrast between China's stated goals and many of the military programs it is undertaking. When put into a context of a rising economic power, China's rise is a cause for closer observation. During testimony before the Senate Armed Services Committee, PACOM commander Adm. Robert Willard concluded that "the scope and pace of its modernization without clarity on China's ultimate goals remains troubling. For example, China continues to accelerate its offensive air and missile developments without corresponding public clarification about how these forces will be utilized."[16] Clearly, Chinese offensive military capability is increasing. Analysis of this rise is necessary to be prepared in the event that Chinese intent or opportunity changes in the future, driving a direct threat against US interests.

Russia

Despite an economic decline following the collapse of the Soviet Union, Russia has maintained a sizeable conventional military force focused on resisting NATO expansion and maintaining influence in Eastern Europe, Central Asia, and the Far East. Within Russia this force is seen as a key to their national strength on the global stage. There is recognition however, that the force requires significant modernization, as much of Russia's military equipment has not been upgraded to keep pace with technological change. To counter this, Russia has embarked on an ambitious program to modernize its forces, invest heavily in military related research and development, and sustain its top tier nuclear forces. In order to achieve these goals a military investment plan was announced in 2008 to reduce the size of conventional forces while focusing on asymmetric, rapid response actions to support Russia's interests. [17]

While Russia's GDP remained stagnant for the 1990s through the mid 2000s, it has increased three fold in the last 10 years[18], and is the world's 7th largest economy at over $2.2 trillion, as measured by purchasing parity.[19] Over the next few decades as global oil supplies

become scarce Russia's petroleum reserves will continue to strengthen the country's economic and political power. Despite this, the Russian Federation is attempting to diversify the economy with focused industrial policy and targeted technology investments.

Russia's "Perestroika" economic restructuring in the 1980s privatized most government-controlled industries but the energy and defense sectors remained under direct government control. Additionally, the Russian government exerts influence on private industry through targeted investments. In order to spur "high tech" growth and diversify the economy, the president of the Russian Federation issued State Science and Technology policy on May 21, 2006 directing a focus on eight specific technology areas.[20] While these areas are the focus of civilian research, all eight areas have a dual use military nature as well.

In 2011 Russia unveiled a $640 billion 10 year military spending plan, $64 billion of which will be dedicated to developing new weapons.[21] In addition to providing a foundation for Russian forces, continued development of advanced weapons for export is a key component of Russia's economic development. This renewed focus on technology investment puts Russia in a position to develop asymmetric, technology based weaponry within the next twenty years. This new weaponry combined with a reduction in conventional troops will result in a future force that relies on asymmetric technological weapons and a sophisticated nuclear arsenal in support of national security objectives.

Limitations

This paper was limited to open source research. Examples discussed are an illustration of the type of asymmetrical military technological capabilities that are being developed. Threats discussed are of a sophisticated, "high end" variety that don't lend themselves to transfer to lesser states or non state actors. Part of this is because the capabilities evaluated leverage

massive, long-term, focused investment to develop the infrastructure required to generate high-end capabilities. Additionally, this paper focuses on the threat side of the equation and does not address known US weaknesses that might be exploited.

---

[4] James Clapper, *Statement for the Record on the Worldwide threat Asssessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence.* Washington, DC: Office of the Director of National Intelligence, 2011,13.
[5] Michael Pillsbury, Michael. *An Assessment of China's Anti-satellite and Space Warfare Policies and Doctrines.* Washington, DC: US-China Economic and Security Review Commission, 2007.
[6] Office of the Secretary of Defense, *Military Power of the People's Republic of China 2007*, 7.
[7] A Sharma, J Page, J Hookway, and R Pannett. "Asia's New Arms Race." *The Wall Street Journal*, February 12, 2011.
[8] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2010,* 18.
[9] Sharma, et al.
[10] Of course this contrasts with US spending of over $680.billion, however, when direct war related operational costs are subtracted, the anticipated Fiscal Year 12 defense spending was $553 billion. US Department of Defense, *Fiscal Year 12 Budget Request.*
[11] People's Republic of China, People's Republic of China. "Defense White Paper 2011" *Information Office of the State Council of the People's Republic of China.* March 31, 2011. http://www.china.org.cn/government/whitepaper/node_7114675.htm.
[12] Economist . "Economics Focus - The year when the Chinese economy will truly eclipse America's is in sight." *The Economist*, December 31st, 2011: 61.
[13] Office of the Secretary of Defense , *Military Power of the People's Republic of China 2007,* 7.
[14] Bill Gertz, *China Blocks Coastal Waters, Enlarges Military.* April 12, 2011. http://www.washingtontimes.com/news/2011/apr/12/china-blocks-coastal-waters-enlarges-military/?page=all.
[15] Office of the Secretary of Defense, *Military Power of the People's Republic of China 2007,* 15
[16] Gertz.
[17] Clapper, 20.
[18] World Bank, World Development Indicators. *Gross Domestic Product - Public data.* http://www.google.com/publicdata/.
[19] Central Intelligence Agency. "The World Factbook, Russia" *The World Factbook, Russia.* January 9, 2012. http://www.cia.gov/library/publications/the-world-factbook/geos/rs.html.
[20] The Federal Targeted Program of "Research and Development in Priority Fields of Russia's S&T Complex for 2007-2012" include 8 areas: Security and Counter-terrorism, Life Sciences, nano systems and nano-materials, Information-Communications Technology systems, Rational Use of Natural Resources, and Energy and Energy Efficiency. Budget over the 5 year period was over $125billion rubles. See http://rp7.ffg.at/upload/medialibrary/80_Burger81299.pdf for more information. Information Society Technologies to Open Knowledge Russia, 14.

[21] Defensetech.org. "Russian Planning 10 Year, $640 Billion Military Modernization." *Defensetech.org.* February 25, 2011. http://defensetech.org/2011/02/25/russia-planning-10-year-640-billion-military-modernization/.

Chinese Information Warfare

The year 2009 was a busy year for China's Information Warfare specialists when they were accused of infiltrating and seizing control of almost 1300 computers in 103 countries belonging to the Dalai Lama and other Tibetan leaders.[22] While definitive attribution was never realized due to the ambiguous nature of the cyber domain, the Chinese were accused of remotely observing data on the compromised computers and of activating cameras and microphones to covertly observe the computers' operators. Given revelations in 2009 that the US's F-35 program office had been attacked and lost terabytes of data, it is clear that even sensitive US government programs are not appropriately protected from malicious cyber activity either.[23] But this is just the beginning of an emerging struggle over information; the Chinese see Information Warfare as much more than cyber attack.

Drawing lessons from US and allied campaigns during the 1991 Gulf War and the war in Kosovo, the Chinese have embarked on a campaign to modernize the People's Liberation Army (PLA) through "Informationization". This focus appears to be an attempt to integrate information across the armed forces to increase efficiency and command and control. China's 2011 Defense White paper calls for "major progress in informationization" by 2020, and within the paper there is a clear focus on "operations under conditions of informationization."[24] From this foundation emerges the Chinese concept of Information Warfare, which does not have an analogous concept in the US. China views Information Warfare as an integrated approach to impact an adversary's information in order to alter perceptions, confuse, or delay action. A significant part of this approach includes information modification, deception, or confusion, based on the historic Chinese precept "hide a knife behind a smile."[25]

To achieve information dominance an informationized PLA will seek to attain mastery of both the electromagnetic spectrum and the global cyber sphere.[26] This approach includes the attempted dominance of air, space, and cyber mediums, through cyber operations, information operations, electronic attack, and kinetic attack on communications and command and control nodes. Writings in Chinese military texts indicate that Information Warfare is a precursor for land or sea dominance, as stated in *Weapons of the 21st Century*, "We must gain air and sea superiority, but win information superiority first of all."[27]

In 2006 the Chinese Communist party released a 15-year development strategy (2006 – 2020) that makes the information domain a priority of the Chinese Communist party.[28] To this end, there is a push within China's professional military schools to assess the utility of military equipment and programs by evaluating the degree to which they support Information Warfare.[29] With a new emphasis on developing Information Warfare, defined in broader terms than the US paradigm of cyber, it is reasonable to expect that China will develop powerful new Information Warfare capabilities that might not be anticipated by the West. Furthermore, the Chinese government has the advantage of experience with Information Warfare concepts that Western governments are lacking due to the Chinese Communist Party's willingness to exercise Information Warfare concepts on its own people.

Within the PLA General Staff Directorate (GSD), an organization called the Third Department is responsible for research, development and operational issues linked to information warfare. The organization is similar to the US's National Security Agency (NSA), but with a broader scope. For technology research and development, the Third Department has institutes that focus on supercomputing, satellite communications, and cryptology. Operationally, the historical mission of the Third Department has been signals intelligence (SIGINT) collection and

analysis. Today, in addition to a robust internal SIGINT network, the Third Department executes computer network exploitation. [30]

Within the computer network area, there are three disciplines: network attack, network defense, and computer network exploitation. When aimed external to China, these methods lead to data exfiltration, data corruption, data manipulation, and even infrastructure damage.[31] The Chinese have long recognized the destructive potential of cyber operations. In 1996, Gen Pan Junfeng, Director of the Foreign Military Studies Department of the Chinese Academy of Military Science wrote that due to US reliance on computer networks "we can make the enemy's command centers not work by changing their data system. We can cause the enemy's headquarters to make incorrect judgments by sending disinformation. We can dominate the enemy's banking system and even its entire social order."[32]

The PLA has also linked cyber network attack and defense with psychological warfare to recognize and counter “misinformation” in cyberspace.[33] The Third Department is believed to be associated with this work which leverages the extensive computer server monitoring and SIGINT capabilities of the organization. In China, psychological warfare and perception management are tightly linked to the Communist Party propaganda effort such that the discipline of information warfare is simply an extension of the natural control of ideas. In the view of the Communist Party, information control, both internal to China and external, is paramount in both wartime and peacetime. [34] Therefore, the holistic concept of information warfare to control ideas, perceptions, and motivations is something that is an ongoing competition between the Chinese government and all adversaries, internal and external.[35]

Conceptually, integration of computer transmissions and electromagnetic spectrum signals recordings onto supercomputers with vast data storage and processing power will provide

the capability to determine the activities of organizations and even people at near real time. Fusion of cell phone, computer, e-mail, radio transmissions, and even satellite spectral imaging will enable the Chinese government to deploy sophisticated non-traditional intelligence, reconnaissance, and surveillance networks with an ever expanding footprint. Even with encryption mechanisms, supercomputing advances will reduce the time required for decryption of coded computer, telecommunications, and radio transmissions. When this capability is linked to the operational experience gained from monitoring and "correcting" information internal to the Chinese state, it can be seen that within the next 25 years the Chinese government will develop information warfare experience and capabilities far exceeding those of Western nations.

Perhaps the most alarming factor with information warfare is the concept of data confusion and deception. There is clear thought to interfering with military command centers and headquarters by changing data in the systems, thus, causing confusion and driving incorrect actions.[36] This type of sophisticated attack has drawbacks in that malicious software will need to be planted ahead of time and the malicious code tends to have only a limited duration of effectiveness. A second challenge is that once activated, it is not clear exactly how or if the code will function and what affect it may have on adversary perceptions.

To remedy the uncertainty of computer based information warfare the Chinese also have plans for more direct, lethal operational concepts in the event of hostilities, under the banner of "integrated network electronic warfare."[37] This tool includes both electronic attack and kinetic attack as methods to disrupt command, control, and communications in an attempt to induce paralysis in an adversary during a military operation. While integrated network electronic warfare is to occur throughout the entire campaign, the emphasis is on the tactical level of attack during the first phases of an operation.[38]

Responsibility for tactical attacks on communications, command, and control nodes falls to both the GSD's Fourth Department and to the PLA Air Force. The Fourth Department is charged with linking computer network attack with the jamming of US satellites.[39] In the future, electromagnetic ground based jamming of US satellites should be expected. For terrestrial targets the Air Force has extensive writings on possible future electronic attacks using anti-radiation missiles, conventional electromagnetic pulse (EMP) bombs, and high powered microwave weapons.[40]

In the future, holistic Chinese information warfare concepts may allow power projection against heavily defended targets or adversaries. Information warfare is seen as an asymmetric capability allowing the "lesser to overcome the greater." The Chinese recognize that many aspects of information warfare can overcome the tyranny of distance that is found in other domains such as air and sea. As a result, there is an asymmetrical advantage that may be gained through heavy investment in information warfare, as the medium can have either regional or long range effects independent of geography for roughly the same cost. [41] The concept of the lesser overcoming the greater even extends to deterrence theory. It is understood that wielding a superior information warfare capability could directly threaten an adversary's homeland even though control of other domains (Sea and Air) might not be on par with the adversary.

Given the Chinese view that there are no distinct boundaries between peacetime and wartime information warfare, and little distinction between internal and external actions, the question is not if information warfare will be used against adversaries, or when an attack might come. Rather, the question is simply what level of conflict is currently occurring? Since deception principles are embedded in information warfare there is no straightforward answer to this question. How does an individual or even a nation detect when they are being deceived or

manipulated? This insidious, pervasive nature is one that will pose a most vexing challenge to China's adversaries over the next 25 years. Due to China's institutional practice of employing information warfare principles on its own people, it will master the capability. There is a clear intent and ongoing actions to employ this capability across the spectrum of conflict. Finally, the opportunity to employ information warfare is practiced on a daily basis and will only increase as the world becomes more electronically integrated.

---

[22] Christopher Ford, *New Paradigms Forum.* February 07, 2011. http://www.newparadigmsforum.com/NPFtestsite/?p=1000.
[23] Sibohan Gorman, AugustCole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *Wall Street Journal.* April 12, 2009. http://online.wsj.com/article/SB124027491029837401.html.
[24] People's Republic of China. "Defense White Paper 2011" *Information Office of the State Council of the People's Republic of China.* March 31, 2011.
[25] Wang Xuanming, *Thirty-Six Strategems.* Singapore: Asiapac Books, 1992, 42.
[26] Stokes, Lin and Hsiao, 2.
[27] As written by Pillsbury "In "Weapons of the 21st Century," Mr. Chang Mengxiong, the former Senior Engineer of the Beijing Institute of System Engineering of COSTIND, suggests "We are in the midst of a new revolution in military technology" and in the 21st century both weapons and military units will be "information-intensified" Pillsbury, "*China Debates the Future Security Environment."*
[28] Mark Stokes, J Lin, and L.C. Hsiao, *The Chinese People's Liberation Army signals Intelligence and Cyber Reconnaissance Infrastructure.* www.project2049.net: Project 2049 Institute, 2011, 2.
[29] Michael Pillsbury, *China Debates the Future Security Environment.* Washington, DC: National Defense Univeristy Press, 2000.
[30] Stokes, Lin and Hsiao , 16.
[31]The trend of convergence of cyber and mechanical devices simply increases the potential for damaging attacks against physical infrastructure James Clapper, *Statement for the Record on the Worldwide threat Asssessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence.* Washington, DC: Office of the Director of National Intelligence, 2011, 27.
[32] Pillsbury, *China Debates the Future Security Environment.*
[33] There is a tension, however, between the PLA and the Communist Party in the capabilities of cyberspace application of Information Warfare and how they should be utilized, particularly on the domestic front. This tension is seen in the recent removal of Lt Gen Wu Guohua from command of the PLA's GSD Third Department cyber force by party leaders. While his specific offense is not understood, it is assessed that he was actively utilizing cyber surveillance and information dissemination internally in a way that caused great alarm within the Party. Stokes, Lin and Hsiao, 6.

[34] In 2003 the Communist Party released the information warfare concept of "Three Warfares" : psychological warfare, media warfare, and legal warfare. Execution of this concept does not have a clear distinction between peacetime and wartime operations, and clearly supports perceived internal and external security threats. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2010,* 26.

[35] In his speech at the National Security Group, Center for Security Policy, Dr Ford discusses the Chinese view of the web and the Chinese concept of information control coming from the Communist Party. In the view of the party, information control is paramount both in wartime and peacetime. As such, a truly free exchange of ideas through American tools like Google and Facebook are seen as threats to the Communist party, and are examples of deliberate American hegemony of the web. Ford, *New Paradigms Forum*.

[36] Pillsbury, *China Debates the Future Security Environment.*

[37] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2010,* 34.

[38] Roger Cliff, John Fei, Jeff Hagen, Elizabeth Hague, Eric Heginbotham, and John Stillion. *Shaking the Heavens and Splitting the Earth : Chinese air force employment concepts in.* Santa Monica: RAND Corporation, 2011,63.

[39] Stokes, Lin and Hsiao, 15.

[40] Cliff, 63.

[41] Center for Strategic and Budgetary Assessments. *Strategy for a Post-Power Projection Era.* Washington, DC: Center for Strategic and Budgetary Assessments, 2010, 42.

Chinese Space Operations

On January 11, 2007 a Chinese ballistic missile intercepted the aging weather satellite Fenyun-1 in a direct ascent head-on collision, instantaneously sending an explosion of over 35,000 shards throughout space.[42] Initially world reaction was muted following Beijing's denials of the operation, but as details came to light the Chinese government admitted the operation was a "successful test". Then US Air Force Secretary Michael Wynne summarized the world's reaction when he stated "We were not surprised; we were shocked." [43] This successful satellite intercept signaled a dramatic shift in the understanding of China's capabilities and intent in space.

A year before the successful anti-satellite test, the 2006 US China Economic and Security Review Commission report foreshadowed China's eventual development of space weapons by publically stating that the PLA's goal appeared to be focused on "obtaining space-related information dominance and the ability to disable its opponents' space assets."[44] The motivation to have the ability to contest control of space is clear, as China recognizes that the key to air control is through space, and "controlling space controls the globe."[45] Due to the belief that space is the "final frontier", in an interview in 2009, the PLA Air Force Commander stated that he saw military competition in space as "inevitable."[46]

China's successful anti-satellite test in 2007 should not have come as a surprise to intelligence analysts. China had previously conducted three other failed anti-satellite tests starting in September 2004.[47] The successful test was simply part of a long, deliberate roadmap to attain control and even dominance of space that traces its roots to space efforts in the early 1990s.[48] During the 2006 commemoration of China's 50 years in space, China's Premier laid

out a vision of unique Chinese innovation and robust research and development in space technologies leading to a manned space station by 2020.[49]

Ascertaining a nation's true military space capability is difficult due to the potential civil-military dual-use nature of many of the technologies and platforms. *Space War,* published by the Chinese National Defense University in 2001 recommends a combination of military and civilian capabilities where civil use capabilities can be used in military applications when needed.[50] While the rationale for dual use activities provides economic efficiency it also shrouds the intent of the program in a cloak of ambiguity.[51] Furthering the challenge is the dual use nature of advanced environmental monitoring constellations, to include synthetic aperture radar, infra-red, and multi-spectral imaging satellites and the fact that Chinese civilian space programs are under PLA control.

Within the ambiguity of both civil and military use satellites, China views space as an extension of the "informationalized" environment. Military doctrine treats space as an extension of the information battlefield resulting in no delineation of space as a distinct theater.[52] For the immediate future, writings indicate that space attack is seen as a method to wage a pre-emptive attack to cause confusion and limit an adversary's ability to react. In the context of the larger information war, space attack is also seen as a capability that could cause doubt in the mind of the enemy commander, possibly preventing an adversary from taking hostile actions in the first place. This might be done either through a demonstration of capability in a deterrent role, or in combination with information warfare, electronic attack, or deception campaigns. No matter the method, a recent article in *China Military Science* concludes, "it is in space that information age warfare will come to its more intensive points." [53]

There's a growing body of evidence that indicates China has dedicated significant thought and resources to developing space denial capabilities. Dr. Michael Pillsbury of the US National Defense University has documented Chinese thought on the weaponization of space through an exhaustive review of twenty three texts, and journal articles. Chinese authors have discussed multiple space attack methods to include direct attack, directed energy, electronic attack, and ground attack of satellite control signals and control stations. Some of the writings advocate the execution of a stealth campaign to develop space control technologies and capabilities outside the view of forgiven observers. These new capabilities could then be deployed as needed at the beginning of a conflict. The concept of stealth in space also extends to the technologies surrounding stealthy space vehicles. Three books published by PLA authors in 2001, 2002, and 2005 discuss the technologies associated with stealth satellites specifically designed to shield both visual light and infrared radiation.[54] This technology would make ground observation and tracking of satellites extremely challenging, potentially protecting satellites from targeting.

Under the direct attack category one of the simplest approaches is to use a high altitude weather monitoring rocket that upon reaching its apogee, releases pellets that fly into the path of a low earth orbit satellite. Even this approach requires precise tracking of the targeted satellite. More sophisticated attack techniques include the combination of multiple technologies. For example, Pillsbury unearthed a recommendation to use submarine anti-satellite weapons to provide a stealthy method to launch microsatellites into low earth orbit (LEO). Once launched these microsatellites could be used to maneuver in close proximity to a target satellite to jam the satellite communications or impact the satellite. A close proximity maneuver capability has already been demonstrated with the recent-orbital BX-1 micro-satellite test carried out as part of

the manned Shenzhou-7 mission.[55] Advanced use of microsatellites in the future could be used for destructive purposes or for more subtle implementation as robotic parasites that rendezvous and interrupt, corrupt, modify, or hijack the target satellite.

A foundation for directed energy interference with satellites has already been set through the development of terrestrial laser tracking systems. Chinese authors have studied US and Russian laser tracking capabilities, noting that Russian ground based lasers have temporally blinded US satellites in the past.[56] Pillsbury also reports Chinese discussion of advanced laser attacks in space to include X-ray lasers, which theoretically would destroy electrical circuitry; however, this type of laser would require either conventional explosives or nuclear weapons to initiate. Chemical Oxygen-Iodine Laser (COIL) in both continuous wave and pulsed modes have also been discussed as having potential for satellite attack.[57]

Under the heading of electronic attack, discussion is focused on jamming of satellite command signals, both from the ground and from space. The most obvious means of ground based interference is through the use of GPS jammers. There is also a bleed over between cyber attack and space attack due to the vulnerability of ground stations and guidance signals. Through cyber, fixed ground stations face hijacking with malicious code, while physically they are susceptible to jamming, sabotage, and even attack from special operations forces. Perhaps the most devastating attack would come from an anti-satellite missile armed with a nuclear or non nuclear electro-magnetic pulse weapon. This type of attack would create an energy wave that would spread to disrupt all satellites in a given orbital track.

Developing potentially asymmetric capabilities in space is a natural strategic approach given the US's overwhelmingly superior conventional forces. Today the United States relies on space assets for both military and economic means to a greater extent than other countries, so

this presents a perfect "Achilles heel" for asymmetric challenge by adversaries.[58] In the future, as China's "informationization" campaign continues, its military capability and commercial sector will also be inextricably linked to space access. As this happens, China will be less motivated to employ a crude space denial strategy. Rather, the strategy will shift a continuous "cat and mouse" conflict to best disrupt its adversaries' space activities while preserving its own.[59]

From a capability standpoint, the assessment is clear: China has a mature space program today, investment in space technology is continuing, and the program will only become more advanced in the future. Furthermore, analysis demonstrates Chinese intent to utilize space based weapons as a natural continuation of the information battlefield. Finally, while demonstrated attacks against space assets have not been widespread, recent revelations that US commercial satellite signals were hijacked in 2007 and 2008 through the exploitation of a ground control station in Norway demonstrates that even today the opportunity exists for malicious activity[60]. The conflict for control of space has already begun.

---

[42] Ashley Tellis, "China's Military Space Strategy," *Survival*, 2007: 41.
[43] Richard Hughes and Jon Lowe. *We Need A Civil Reserve Space Fleet.* March 2008. http://www.au.af.mil/au/aunews/archive/2008/0307/Articles/CivilReserveSpaceFleet.htm.
[44] The goal of this was to "disrupt their (the adversary's) space-based information and navigation systems in the event of conflict" Pillsbury, *Assessment of China's Anti-satellite and Space Warfare Policies and Doctrines*, 8.
[45] Michael Pillsbury, *China Debates the Future Security Environment.* Washington, DC: National Defense Univeristy Press, 2000.
[46] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2010,* 4.
[47] Tellis, 43.
[48] Ian Easton, Ian. "The Great Game in Space." *Project 2049 Institute.* http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf, 2.
[49] Office of the Secretary of Defense.
[50] Pillsbury, *Assessment of China's Anti-satelliteand Space Warfare Policies and Doctrines,* 11.
[51] This ambiguity has unfortunate negative consequences on verification efforts should there be any sort of space treaties. Analysis by Ashley Tellis indicates that a space treaty is not likely due

to the Chinese view that it is the last "strategic frontier" where they see the potential to rival the US without directly confronting the US's overwhelming superior conventional forces. Due to the apparent inevitability of the weaponization of space, US Sen Jon Kyl from Arizona concludes that the path forward is to develop US offensive counter-space capabilities in order to deter China's space weapons build-up.

[52] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2010,* 25.

[53] Larry Wortzel. "The Chinese People's Liberation Army and Space Warfare." *Astropolitics*, 2008, 115.

[54] Pillsbury, *Assessment of China's Anti-satellite and Space Warfare Policies and Doctrines,* 5

[55]In this test the BX-1 microsat was utilized as a surveillance platform where it executed multiple rendezvous with the manned capsule. (Weeden 2008).

[56] Pillsbury, *Assessment of China's Anti-satellite and Space Warfare Policies and Doctrines*, 27.

[57] Ibid., 46.

[58] Tellis, "China's Military Space Strategy," 48.

[59] Wortzel, 125.

[60] In October and July 2008 the Landsat-7 earth observation satellite system experienced interference and hackers also interfered with a Terra AM-11 earth observation satellite in 2008. See http://smallwarsjournal.com/blog/china-suspected-in-cyber-attacks-on-us-satellites.

Russian Nuclear Weapons

In 2010 Russian President Vladimir Putin released updated military doctrine of the Russian Federation, the first public update to doctrine since 2000. This new doctrine contained subtle wording changes that deemphasized nuclear weapons employment, however there is a level of ambiguity that has led to debate as to the actual intentions of the Russian state with regard to nuclear weapons. Russian actions and statements about nuclear research and development over the last ten years point to a robust program of design and testing that is focused on developing an entirely new class of weapons. Ongoing physics research has resulted in the emergence of a new set of "fourth-generation" nuclear weapons technologies not covered by the Comprehensive Test Ban Treaty (CTBT).[61] These weapons promise to introduce exquisite low yield weapons within the next 20 years. New weapons combined with a Russian theory of limited use of nuclear weapons as a method of "de-escalation" points to a more aggressive posture than the one signaled in Russia's written doctrine.

The newest doctrine of the Russian Federation states "Nuclear weapons will remain an important factor for preventing the outbreak of nuclear military conflicts and military conflicts involving the use of conventional means of attack (a large-scale war or regional war)".[62] The doctrine goes on to state that nuclear weapons may be utilized during a conventional conflict should there be a threat to the existence of the state. In other words, there is no inhibition against first use of nuclear weapons. This new doctrine, at least, places less emphasis on nuclear weapons than the doctrine from 2000 that envisioned the use of nuclear weapons "in situations critical for national security".[63] Recently, however, Deputy Prime Minister Sergei Ivanov has stated that there is no difference between the 2010 and 2000 versions of the doctrine with respect to nuclear weapons.[64] Regardless of any wording change, the Russian Federation views nuclear

weapons as a vital capability to maintain prominence on the world stage following the collapse of Soviet Union. To address the perceived threat from the NATO alliance and other regional neighbors, tactical nuclear weapons provide an opportunity for parity given reduced conventional force capabilities.

In 1999 the concept of "de-escalation" through the use of nuclear weapons was introduced by a group of officers led by Major-General V.I. Levshin writing that "fulfilling the de-escalation concept is understood to mean actually using nuclear weapons for both showing resolve as well as for the immediate delivery of nuclear strikes against the enemy."[65] This new willingness to use nuclear weapons was dependent on development of new generations of low yield weapons. Further writing on the subject revealed the logic that "it is assumed that a precision strike of this kind will not result in immediate nuclear war."[66] Ultimately, this approach extends Russian use of nuclear weapons from one of strategic deterrence to one that enables a global influence through the threat of precision low yield tactical nuclear weapons.

There is clear evidence that a first use of tactical nuclear weapons has been considered in the past and that the Russian armed forces continue to train and deploy for such an action. Five years after the conflict, for example it was revealed that the Russians had considered the use of nuclear weapons in response to NATOs efforts in Kosovo in 1999.[67] Russian armed forces have a long history of exercises in which ground and air forces employ nuclear weapons as a first strike weapon when confronted with conventional forces on the Russian border. Delivery methods contemplated include Submarine Launched Cruise Missiles (SLCMs) and Air Launched Cruise Missiles (ALCMs) from Tu-95 and Tu-160 bombers.[68,69] Recent Russian Defense Ministry press releases indicate continued deployment of SLCMs with nuclear warheads and

deployment of nuclear weapons with the Troop and Artillery arms of the Russian Ground Troops.[70,71]

Within the intelligence community there is debate as to the scope of Russian nuclear weapons testing. There continues to be a high level of activity at the Hovaya Zemlya test site north of the Arctic Circle, reportedly employing over 4,000 people. [72] In the open press there have been discussions of "hydronuclear" experiments leading to "subcritical" yields.[73] While the tests are conducted under the intent of determining stockpile safety under the CTBT, they also provide the benefit of providing a pathway for improved warheads and the development of new weapons types.

There are wide press reports of continued Russian development of nuclear technologies, and in January 2005 Russian Defense Minister Sergei Ivanov stated "New types of nuclear weapons are already emerging in Russia."[74] The exact weapons types are not clear, but advances in nuclear physics combined with emerging nanotechnology and advanced lasers point to development of a new class of low yield (1 to 100 ton) "fourth generation" weapons, a radical departure from the kiloton to megaton nuclear weapons of today. These weapons will enable precise shape charged jets and increased prompt radiation effects with reduced collateral damage and minimal secondary radioactivity.[75] Through the use of a deuterium-tritium (DT) fusion reaction these weapons will be able to produce a 1 ton explosive yield with as little as 25mg of fissile material, enabling extremely compact weapons.[76]

Two technology sets are being worked on that are likely to drive the development of low yield nuclear weapons. The first is development of DT fuel pellets for use as fissile material. Ongoing efforts in this area are being pursued by many countries to include Russia. DT fuel promises to provide a new fuel for nuclear power generation that provides a more compact and

continuously adjustable energy source.[77] Today there is experimentation on DT fuel using Internal Confinement Fusion where the fuel is compressed by lasers in a laboratory environment. In support of this research, Russia has embarked on building the world's largest laser facility with a planned power of 2.8 million Joules of ultraviolet laser energy.[78] Laboratory experimentation on DT produces radiation but does not require explosive testing and is not subject to the CTBT.[79] DT fueled nuclear power technology is expected to be mastered within the next decade.

The second, more challenging technology set required to weaponize DT fuel is development of a compact trigger component. Again, a number of countries including Russia are conducting research into areas to include pentawatt "super lasers", nuclear isomers, magnetic explosion, chemical laser initiators, and even antimatter triggers.[80] While the timeline for successful packaging of DT fuel with a compact trigger source is not clear, any nation that is successfully able to integrate these technologies will have developed a powerful new capability to create low yield, scalable, "clean" nuclear weapons.

We are entering an era where there is an equalization of the effects between tactical nuclear weapons and conventional non nuclear weapons. The challenge over the next twenty years will be a balance between conventional weapons achieving "nuclear effects" versus the continued development of new forms of nuclear weapons. Nations are likely to take different approaches, and herein lies the problem of nuclear weapons. Since Russia recognizes it can't afford to develop and maintain a non nuclear capability on par with the United States, militarily it must embrace the capabilities of tactical nuclear weapons as a hedge against US conventional force dominance. Given Russia's relatively low threshold for nuclear weapons employment, the

looming conflict over control of information may lead to a dangerous escalation from continuous conflict in domains of space and cyberspace to that of a nuclear war.

---

[61] First generation fission weapons were developed in the 1940s, 2nd generation fission-fusion "thermonuclear" weapons were developed in the 1950s, 3rd generation tailored effect weapons such as "neutron bombs" and EMP weapons were developed in the 1960s through 1980s. 4th generation low yield weapons research is ongoing today.

[62] Russian Federation, . "The Military Doctrine of the Russian Federation." *SRAS.org.* February 5, 2010.

[63] Nikolai Sokov, "The New 2010 Russian Military Doctrine: The Nuclear Angle" *Center for Nonproliforation Studies, Monterey Institue of Interational Studies.* February 5, 2010.

[64] Mark Schneider, "The Nuclear Forces and Doctrine of the Russian Federation." *Comparative Strategy*.

[65] The writings state "It seems to us that the cessation of military operations will be the most acceptable thing for the enemy in this case" Schneider, 411.

[66] Ibid., 414.

[67] Ibid., 401.

[68] A nuclear weapon is composed of two parts, the warhead and the delivery system. Strategic nuclear weapons treaties have inspection mechanisms set to monitor the number of delivery systems and deployed warheads, while the total number of warheads to include those in storage is subject to less scrutiny. Under this framework any treaty on tactical nuclear weapons will be much more challenging to implement due to the inherent dual use capability of tactical nuclear weapon delivery systems. Estimates of Russia's stock of tactical nuclear weapons vary, with a low end estimate of approximately 2000. Schneider, 401-403.

[69] Nikolai Sokov, "A Second Sighting of Russian Tactical Nukes in Kaliningrad." *Center for Nonproliforation Studies, Monterey Institue of International Studies.* February 15, 2011.

[70] Schneider," 409.

[71] There is also speculation that the newest Russian Iskander ground missile system with a range of 500 kilometers is capable of nuclear weapons delivery. Sokov.

[72] Schneider, 409.

[73] Depending on the structure of the test, compliance with the Comprehensive Test Ban Treaty is debatable. William Broad and Patrick Tyler. "Dispute over Russian Testing Divides US Nuclear Experts." *New York Times.* March 4, 2001.

[74] Schneider, 398.

[75] Andre Gsponer, *Fourth Generation Nuclear Weapons: Military Effectiveness and Collateral Effects.* Geneva: Independent Scientific Research Institute, 2008, 1.

[76] Ibid., 2.

[77] Ibid., 12.

[78] Nizhny Novgorod, Nizhny. *Russia Set to Build World's Most Powerful Laser Station.* February 9, 2012.

[79] Jason Wood, Jason. "Forth Generation Nuclear Weapons: Moving the Nuclear Debate Beyond Fission." *csis.org.* March 27, 2009.

[80] Gsponer, 12.

Conclusion

We are in the midst of a shift in strategic eras from the traditional American way of war through mass and dominance to an ambiguous state of constant conflict over information. The nature of the new global commons of space and cyberspace will have a leveling effect where parity between world powers is inevitable. In this new era, the effectiveness of today's conventional global strike will be reduced to the point where it is of limited deterrence value. The US must recognize that it will not be able to control the new domains of cyber and space as it has enjoyed the control of the sea and air, and must appropriately prepare for this new reality.

US vulnerability to information warfare through the commons of space and cyberspace is acknowledged by today's military leaders. With respect to the role cyberspace plays in security operations, US Pacific Command Commander Admiral Robert Willard recently admitted to the Senate Armed Services committee "I depend entirely, nearly, on cyberspace for the command and control of the broader Asia-Pacific, of our forces there".[81] In the space realm, following the 2007 Chinese ASAT test, Lieutenant General Mike Hamel, Space and Missile Systems Center concluded "If they take our asymmetric advantage in space, we go from an information age war machine to an industrial age war machine, shifting that balance, the edge will go to the adversary."[82]

The new US national military strategy released in January 2012 is a step in the right direction. A renewed emphasis on cyber and space capabilities should be pursued. The US should prepare for the effects of robust information warfare, space warfare, and nuclear capabilities and should evaluate how these three areas might be combined together to produce overwhelming effects. Additionally, as the effectiveness of conventional global strike becomes

diminished, the implications that this new era of parity will have on deterrence theory must be closely examined.

Even the emergence of a new tri-polar reality dominated by the US, China, and Russia will only last for so long. In the far future, once the transition to a true form of information warfare occurs, nuclear weapons will become less important. There will be a continuous level of conflict, and the tenet that possession of nuclear weapons is a deterrent force in itself will break down. When ambiguity and parity replace deterrence, the relative power of states will be flattened through an explosion of capabilities of peer or near peer states. India, Japan, Iran, European nations, and even non state actors will enter into competition to control information based on their ability to generate the human capital as the means to operate in the conflict over information and ideas.

For the immediate future, however, should China or Russia make significant strides in any of the analyzed technologies at a rate greater than that of the US, the US will be placed at a strategic disadvantage. Due to technological developments, through information warfare and space operations backed up with the deterrent effect of nuclear weapons, China and Russia will gain in national power and ability to directly threaten US interests on a global spectrum. Given the superiority of the US's conventional forces, other nations will naturally focus on asymmetrical capabilities to gain strategic advantage. Due to their significant infrastructure matched with a doctrinal emphasis on aggressive use of space, cyberspace, and nuclear weapons, the threat of an information warfare conflict with China and Russia should not be taken lightly. The chilling reality is that both China and Russia have extremely low thresholds to apply new space, cyber, and nuclear capabilities across the full spectrum of conflict. This shift to an era of continuous conflict over information in the space and cyberspace domains can be anticipated and

should be prepared for in order to counter erosion of US power during the emergence of a new tri-polar world.

---

[81] Bill Gertz, *China Blocks Coastal Waters, Enlarges Military.* April 12, 2011.
[82] Hughes and Lowe.

Bibliography

Apte, Uday, and Hiranya Nath. "Size, Structure and Growth of the US Information Technology." January 2004. http://www.anderson.ucla.edu/documents/areas/ctr/bit/ApteNath.pdf (accessed January 28, 2012).

Broad, William, and Patrick Tyler. "Dispute over Russian Testing Divides US Nuclear Experts." *New York Times.* March 4, 2001. http://www.nytimes.com (accessed January 18, 2012).

Center for Strategic and Budgetary Assessments. *Strategy for a Post-Power Projection Era.* Washington, DC: Center for Strategic and Budgetary Assessments, 2010.

Central Intelligence Agency. "The World Factbook, Russia" *The World Factbook, Russia.* January 9, 2012. http://www.cia.gov/library/publications/the-world-factbook/geos/rs.html (accessed January 21, 2012).

Clapper, James. *Statement for the Record on the Worldwide threat Asssessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence.* Washington, DC: Office of the Director of National Intelligence, 2011.

Cliff, Roger, John Fei, Jeff Hagen, Elizabeth Hague, Eric Heginbotham, and John Stillion. *Shaking the Heavens and Splitting the Earth : Chinese air force employment concepts in.* Santa Monica: RAND Corporation, 2011.

Defensetech.org. "Russian Planning 10 Year, $640 Billion Military Modernization." *Defensetech.org.* February 25, 2011. http://defensetech.org/2011/02/25/russia-planning-10-year-640-billion-military-modernization/ (accessed November 12, 2011).

Easton, Ian. "The Great Game in Space." *Project 2049 Institute.* http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf (accessed January 28, 2012).

Economist . "Economics Focus - The year when the Chinese economy will truly eclipse America's is in sight." *The Economist,* December 31st, 2011: 61.

Ford, Christopher. *New Paradigms Forum.* February 07, 2011. http://www.newparadigmsforum.com/NPFtestsite/?p=1000 (accessed January 24, 2012).

Gertz, Bill. *China Blocks Coastal Waters, Enlarges Military.* April 12, 2011. http://www.washingtontimes.com/news/2011/apr/12/china-blocks-coastal-waters-enlarges-military/?page=all (accessed February 1, 2012).

Gorman, Sibohan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter-Jet Project." *Wall Street Journal.* April 12, 2009. http://online.wsj.com/article/SB124027491029837401.html (accessed February 11, 2012).

Gsponer, Andre. *Fourth Generation Nuclear Weapons: Military Effectiveness and Collateral Effects.* Geneva: Independent Scientific Research Institute, 2008.

Hughes, Richard, and Jon Lowe. *We Need A Civil Reserve Space Fleet.* March 2008. http://www.au.af.mil/au/aunews/archive/2008/0307/Articles/CivilReserveSpaceFleet.html (accessed January 30, 2012).

Information Society Technologies to Open Knowledge Russia. "ICT in Russia: R&D Priorities, Current Situation, Trends, and Forecasts." *Informatin Society Technologies to Open Knowledge Russia.* www.istok-ru.eu/files/Biblioanalysis_ISTOK_Eng_0.pdf (accessed November 16, 2011).

Manea, Octavian. *Interview with Jim Thomas.* June 10, 2011. http://smallwarsjournal.com/blog/journal/docs-temp/789-manea.pdf (accessed January 30, 2012).

Novgorod, Nizhny. *Russia Set to Build World's Most Powerful Laser Station.* February 9, 2012. http://en.ria.ru/world/20120209/171236043.html (accessed February 10, 2012).

Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China.* Washington, D.C.: Department of Defense, 2011.

Office of the Secretary of Defense. *Military Power of the People's Republic of China.* Washington, DC: Office of the Secretary of Defense, 2007.

People's Republic of China. "Defense White Paper 2011" *Information Office of the State Council of the People's Republic of China.* March 31, 2011. http://www.china.org.cn/government/whitepaper/node_7114675.htm (accessed January 21, 2012).

Pillsbury, Michael. *An Assessment of China's Anti-satellite and Space Warfare Policies and Doctrines.* Washington, DC: US-China Economic and Security Review Commission, 2007.

Pillsbury, Michael. *China Debates the Future Security Environment.* Washington, DC: National Defense Univeristy Press, 2000.

Russian Federation. "The Military Doctrine of the Russian Federation." *SRAS.org.* February 5, 2010. http://www.sras.org/military_doctrine_russian_federation_2010 (accessed January 12, 2012).

Schneider, Mark. "The Nuclear Forces and Doctrine of the Russian Federation." *Comparative Strategy*, 2008: 397-425.

—. "Written Testimony - Nuclear Forces and Doctrine of the Russian Federation and the People's Republic of China." *US House Armed Services Subcommittee on Strategic Forces.* October 14, 2011. http://armedservices.house.gov/index.cfm (accessed February 5, 2012).

Sharma, A, J Page, J Hookway, and R Pannett. "Asia's New Arms Race." *The Wall Street Journal*, February 12, 2011.

Sokov, Nikolai. "A Second Sighting of Russian Tactical Nukes in Kaliningrad." *Center for Nonproliforation Studies, Monterey Institue of International Studies.* February 15, 2011. http://cns.miss.edu/stories/110215_kaliningrad_.htm (accessed January 18, 2012).

—. "The New 2010 Russian Military Doctrine: The Nuclear Angle." *Center for Nonproliforation Studies, monterey Institue of Interational Studies.* February 5, 2010. http://cns.miis.edu/stories/100205_russian_nuclear_doctrine.htm (accessed January 10, 2012).

Stokes, m, J Lin, and L.C. Hsiao. *The Chinese People's Liberation Army signals Intelligence and Cyber Reconnaissance Infrastructure.* www.project2049.net: Project 2049 Institute, 2011.

Tellis, Ashley. "China's Military Space Strategy." *Survival*, 2007: 41-72.

Toffler, Alvin, and Heidi Toffler. *War and Anti War.* Boston: Little, Brown, and Company, 1993.

US Department of Defense. *Fiscal Year 12 Budget Request.* February 2011. http://comptroller.defense.gov/budget.html (accessed February 11, 2012).

Weeden, Brian. *The Space Review.* October 8, 2008. http://www.thespacereview.com/article/1235/1 (accessed February 11, 2012).
Wood, Jason. "Forth Generation Nuclear Weapons: Moving the Nuclear Debate Beyond Fission." *csis.org.* March 27, 2009. http://www.csis.org/images/stories/poni/090401_wood_fourth_generation.pdf (accessed February 5th, 2012).
World Bank, World Development Indicators. *Gross Domestic Product - Public data.* http://www.google.com/publicdata/ (accessed 01 22, 2012).
Wortzel. "The Chinese People's Liberation Army and Space Warfare." *Astropolitics*, 2008: 112-137.
Xuanming, Wang. *Thirty-Six Strategems.* Singapore: Asiapac Books, 1992.