The Advanced Tactical Fighter, The Joint Strike Fighter and Information Warfare: Opportunities and Challenges to American Air Dominance in the 21st Century

Captain Gilberto Rosario (USAF),
694th Intelligence Group, Air Intelligence Agency,
Fort George G. Meade, Maryland 20755

Abstract

America's dominance of the skies above the battleground provides our troops the freedom to operate in enemy territory while at the same time denying our adversaries their airspace. To continue to maintain this dominance, the US is faced with the need to modernize its fighter fleet in times of fiscal austerity. To attain this goal, the US is investing heavily in state-of-the-art technologies such as stealth and advanced integrated avionics. These technologies are highly dependent on Information Systems to succeed. Information Systems can exploit Information Warfare (IW) or become vulnerable to it. The purpose of this paper is to explore how our current modernization programs may be affected by IW and the impact this could have in the National Security Strategy . The Scope of this paper is to address only information systems on which the Advanced Tactical Fighter (ATF) and Joint Strike Fighter (JSF) aircraft directly depend to perform their mission.

1. Introduction

Our National Security Strategy is always compared to and influenced by our constitution*: "provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our posterity"*.[1] These principles influence the President's vision in the National Strategy called "Shape, Respond, Prepare Now".[2] Derived from this, the National Military Strategy describes the strategic environment and the national military objectives, also identifies military capabilities required.[3] This document is of paramount importance. It provides high level guidance to the Armed Services on what the National Objectives are. The Armed Services then develop their plans to support the national goals.

It is interesting to note that these documents not only provide the national goals and vision but also make specific reference to asymmetric challenges we will face, among them IW.[4] The ATF and JSF programs are vital to our National Strategy. These two programs seek to replace our fast aging fleet of fighter aircraft. The Air Force F-15 Eagle, our current air superiority fighter is rapidly approaching the end of its service life.[5] The JSF program, a more ambitious one, seeks to replace a wide range of military airplanes with the added challenges of producing a multi-service, multinational airplane that can satisfy multiple requirements and still be affordable in today's diminishing defense budgets.[6] To tackle these challenges, the United States is making an enormous investment in state-of-the-art technologies that will enable these platforms to deliver unprecedented performance within fiscal austerity. These weapon systems are heavily dependent on advanced Information Systems.

2. The Advanced Tactical Fighter

The ATF has been under development since 1984. It is the result of an early 1980s study to identify a successor to the venerable F-15 Eagle. The ATF was conceived to be not just a replacement for the Eagle but a revolution in military aviation.[7] To maintain this dominance, the Air Force embarked on a voyage to make the ATF the most advanced fighter in the world. Its onboard computer systems make it a flying computer network. The combined computing power of this airplane is roughly equivalent to two Cray supercomputers.[8] The high level of integration on its avionics suite provides the pilot with unprecedented situational awareness. The pilot will be able to "see first, shoot first and kill first".[9] The airplane capabilities go well beyond those of a contemporary fighter. It is a fourth generation stealth aircraft, allowing the pilot to penetrate heavily defended areas with little or no probability of being detected.[10]

This enhanced effectiveness can only be attained by massively integrating all its electronic functions on its computers. Without its internal computer network, the airplane will be just an airframe with two engines and low observable physical characteristics. This situation presents a unique dilemma. The aircraft will be incredibly powerful; its computer network fuses multiple data sources into a synthesized display for the pilot. This characteristic is likely to remain unmatched by any potential adversaries well into the next century.[11] However its complete dependence on its internal computer network as well as on the ground support systems make it a target to potential IW attacks. This issue is enormously important for the US not only in military terms but also, at a higher level for the successful execution of our National Strategy.

2.1 The ATF Information Systems

The ATF flies with a maximum of six Advanced Avionics Communications Security (COMSEC) Units (AACU) known as KOV-5s.[12] These are specially developed computers. These computers are integrated into the Common Integrated Processor (CIP), a liquid cooled device. The KOV-5s are computers capable of performing multiple avionics and traditional COMSEC functions simultaneously. The CIP, developed by the Hughes Aircraft Company has a general processing capacity of 9 billion operations per second and 340 million instructions per second.[13]

The ATF incorporates highly integrated avionics for a single pilot operation. The CIP handles all the avionics functions, including self-protection countermeasures and radios. The CIP system automatically reconfigures to compensate for faults or equipment failure. The CIPs also possess growth provisions for infrared search/track. The aircraft CIPs are connected through a 400 Mbits per second fiber-optic network.

In the ground, the ATF is assisted by a dizzying array of computer networks providing, mission planning, maintenance and training systems to name a few. This unprecedented integration is extremely complex. Additionally, once airborne, the ATF interfaces with a wide variety of computer based systems such as the E-3 Airborne Warning and Control System (AWACS) aircraft and Global Positioning System (GPS) Satellites. These data sources are vital to the situational awareness of ATF.

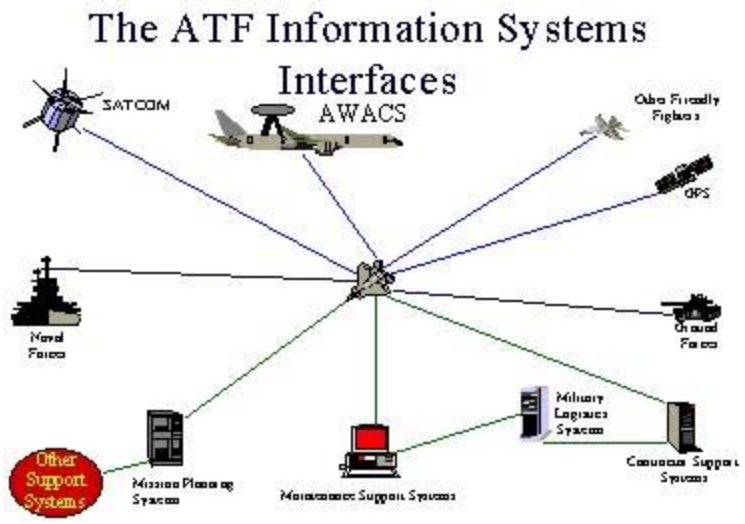


Figure 2-1

As we can see, the complexity of these systems and the impact they have between each other is astonishing. This unprecedented integration of systems makes the ATF a powerful weapons platform. Unfortunately, the commonly known computer systems vulnerabilities to viruses and other malicious attacks are a source of great reason for concern to the ATF.

To exacerbate this problem, today the Department of Defense (DoD) moves away from traditional custom made information systems towards commercially available products.[14] This change in the DoD acquisition practices strives to maximize return on defense investments by taking advantage of commercially available systems. As a result, many of the commercial systems bring in security vulnerabilities normally not found in systems originally designed for military use. Many of these information systems weaknesses are widely available to anyone with access to publicly available information sources like the Internet.[15] These open sources and the fact that we acquire these commercial systems makes it easier for our adversaries to gather intelligence on ways to attack weapon systems like the ATF.

3. The Joint Strike Fighter

Formerly known as Joint Advanced Strike Technology (JAST), the JSF program is perhaps the most challenging acquisition program ever attempted. This program seeks to satisfy the following requirements: low cost, multi-role fighter to replace the F-16 and A-10 for the Air Force, first-day-of-the-war survivable strike aircraft for the Navy, replacement for the Marine Corps AV-8 Harrier and F-18, and replacement for the United Kingdom Royal Navy FA-2 Sea Harrier.[16] Current estimates for acquisition place the total production number in approximately 3,000 units with potential sales to other foreign countries beyond that number. The JSF acquisition program is different from the ATF because the ATF fighter was not originally developed for export sales. In addition, given current emphasis placed in coalition and joint operations, the JSF program must produce an aircraft that shares many common technologies with each service and allies.[17] This goal opens the information systems of the JSF program to more threats and vulnerabilities when compared to the ATF.

JSF will be the compliment to the ATF like the F-16 is today to the F-15.[18] The ATF will clear the skies so air and ground operations could proceed with minimum or no risk to our forces. The JSF will perform other missions like close air support. JSF and the ATF, as force applicators for the US and our coalition friends and allies will depend both heavily on information systems to operate.[19] This situation presents a challenge to US military planners. Coalition warfare and highly integrated information systems are environments that raise serious concerns not present in unilateral operations. The potential vulnerabilities of conducting allied or coalitions warfare were recognized many years ago by Clausewitz in his masterpiece, "On War".[20]

3.1 The JSF Information Systems

JSF seeks to maximize on the foundation work the ATF program laid. This approach, to try to transfer as much technology as possible from the ATF program to JSF aims at attaining a big return from the defense dollar. This approach however, is not free from challenges. Although transferring technology from one program to another makes sense it could also bring new security concerns. Sharing technology with JSF could expose the ATF technologies to additional foreign threats not present in a national program.

JSF will move towards the route already taken by the ATF program, advanced integrated avionics. Among many key technology maturation programs in JSF we find advanced diagnostics, integrated radio frequency systems, integrated core processing and software and other equally dependent technologies on information systems.[21]

Employment of JSF assets around the globe will support National Strategy and objectives. In this respect, JSF will be part of power projection and overseas presence to communicate potential adversaries our intentions.[22] Consistent with this, and the Chairman of the Joint Chiefs of Staff (CJCS) vision of military power based on information superiority and technological innovation, this platform will be equally capable of operating low intensity conflicts as well as in full fledged war.[23] JSF will be part of a decisive force from day one, superior to any adversary. This will be possible by including all-source intelligence data from satellites and airborne platforms among many. Like the ATF, JSF will have to interact with these information systems that represent a force enhancement as well as a potential vulnerability.

The JSF program is currently on its Concept Demonstration Phase (CDP). In this respect, the weapon system computer information architecture is not mature yet. This architecture can be modified to resist IW attacks, a more challenging task in the much more developed ATF. At this early stage, the JSF program has a preliminary weapon system information architecture.

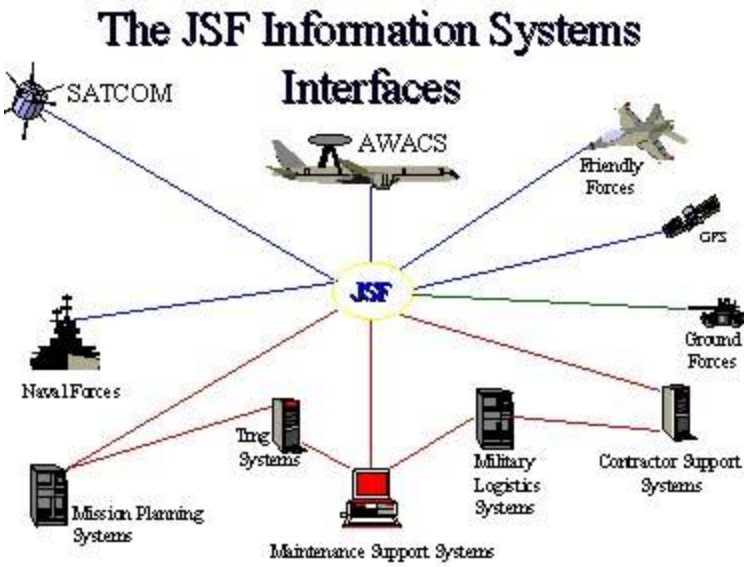


Figure 3-1

This Weapon System description presents a clear picture facilitating the understanding of the program's information systems employment. This picture looks very close to what the ATF weapon system is today (See Figure 2-1).

Regardless of the final architecture and configuration of the information systems it is certain that the program will follow current DoD directives to maximize the value of commercially available products and technologies.[24] This acquisition approach presents a challenge to secure our weapons systems information from external threats and insiders alike. Unfortunately, the features that often make commercial information systems technology attractive also bring considerable security concerns.

4. Information Warfare

IW importance and increased awareness among DoD components is driven in part by computer security incidents in recent memory.[25] IW, however, is not clearly understood by many and it is not consistently defined across DoD.[26] IW is in fact, a sub-discipline of the broader Information Operations (IO).

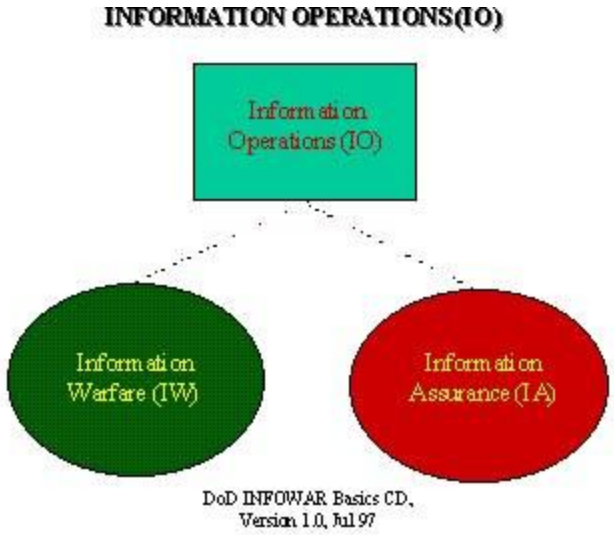


Figure 4-1

It is important to define IW to engage in further discussion regarding this complex and yet evolving concept. As a sub-discipline of Information Operations[27] IW is defined as: *"information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries".*[28] IW is part of a larger group of INFOWAR disciplines.[29]

Figure 4-2

These different categories range from traditional concepts like deception to current IW attacks to computerized information systems. IW importance to ATF and JSF can be illustrated in the following picture.

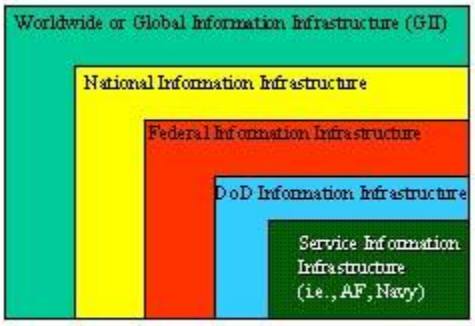
Figure 4-3

As we can see, these weapon systems are totally dependent on internal or external computer systems. Without many of them, they are severely impaired or inoperable.

1. IW, The ATF, JSF and Global Information Infrastructures (GII)

To better understand the complexity of the infosphere where ATF and JSF will operate we have to first take a top view of the global information infrastructures and how these two weapon systems will operate within them. The following illustration shows how different information infrastructures are interrelated and the importance they could have on ATF and JSF.

A Top Level View of Different Information Infrastructures



Adapted from Keith V. Porter, An Analysis of Unclassified Current and Pending Air Force Information Operations Doctrine and Policy, AFIT, Dec 1997

Figure 4-4

JSF and the ATF will be dependent upon these different information infrastructures to operate. This new paradigm could be seen like a new dimension on warfare, equivalent in importance and complexity to conducting sea or land based operations. Without these infrastructures our weapon systems become much less capable.

As we move more towards dependence in openly available, commercial technologies, the weapon systems will also depend on them to operate on each one of the infrastructures as well as to switch between them. This new paradigm is currently a challenge that will persist into the next century: How to take advantage of this extraordinary medium while doing it safely, without compromising our military's ability to carry out the National Strategy. As we will see, the security challenges that lie ahead are very complex and difficult, the opportunities enormous.

4.2 IW as a Complement to Integrated Weapon Systems

IW can be characterized as a double edged sword. If exploited properly it has the potential to become the greatest force multiplier. If left unchecked, it can spell defeat to our military forces. The Air Force has already recognized the utility of IW. On its "New World Vistas" study the Air Force states: *"It should be the goal of the Air Force to achieve information dominance to enable the execution of its missions through the unconstrained but protected use of the infosphere, including segments that the Air Force does not control".*[30] This statement clearly recognized that in order to be effective, the Air Force will have to engage in IW activities at all levels of the GII. This recognition has profound implications because of the added value of IW to future air operations. These two acquisition programs will certainly enjoy the benefits IW can offer as force multiplier and protector.

It is possible to exploit the infosphere and carry out an IW preemptive strike on our adversaries. This could leave them paralyzed at the beginning of the conflict, unable to sustain any military operations of significance at all. The results could be similar to those from the air attacks on Iraq's C3 systems the first day of Desert Storm. This is a good example of how IW can be used to assist and protect our forces.

Malicious Computer Code could be used as a weapon.[31] Some models have been developed on how to employ computer code as a weapon. The following figure is an example.

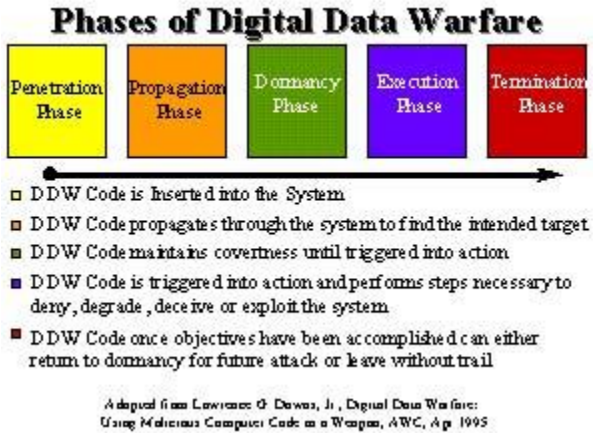


Figure 4-5

Wyatt C. Cook, on his research paper "*Information Warfare: A New Dimension in the Application of Aerospace Power"* argues that IW can be used at all three levels of war, tactical,

operational, and strategic.[32] This type of employment of IW attacks on the enemy can be another example of force enhancers and protectors. For example, IW could disable the enemy's information systems, military and non-military. This can disrupt his effective use of information systems for command and control. A situation like this will allow our forces to operate with ease and impunity. If the same IW attacks were to be performed at a strategic level, they may allow us to neutralize all the enemy information infrastructure with the possibility of forcing them to make concessions without the employment of our military assets. This could be the ultimate force protection since this could make it unnecessary to commit aircraft to combat.

4.3 IW as a Threat to the ATF and JSF

Threats come from a range of sources-from individuals (unauthorized users or insiders) to complex national organizations (foreign intelligence services and adversary militaries). Boundaries between these groups are indistintic, and is often difficult to discern the origins of any particular incident. For example, actions that appear to be the work of hackers may actually be the work of foreign intelligence services. Sources include unauthorized users, insiders, terrorists, nonstate groups, foreign intelligence services, and opposing militaries or political opponents.[33]

As a complex computer network, the ATF could be vulnerable to computer attacks. The JSF, a fifth generation fighter aircraft in the same category that the ATF is could be vulnerable too. They depend on complex computer network systems to fully exploit the power of their own computer systems. To make this possible, these systems need to interconnect and share data. To do this effectively systems need to be standardized. This standardization of technology for effectiveness and economies tends to standardize the vulnerabilities available to our adversaries.[34] Interoperability and standardization have enormous implications to the ATF and JSF programs. The paradox is that in order to deliver the performance sought by the services the systems need to interface with other platforms to acquire and share information, this makes them potential targets of IW attacks directed to them or these platforms.

Current initiatives in the DoD seek to develop a Common Operating Environment (COE) and a Shared Data Environment (SHADE) where all our military assets will share the same foundation for C4I.[35] This initiative seeks to integrate Database Utilities, Distributed Computing Services, Data Interchange Services, Data Management Services and Software Engineering Services for all the users across the Defense Information Infrastructure (DII). There are many commercially available components that form part of this initiative. Some examples are: Oracle™, Sybase™, Informix™ and Microsoft™ databases that operate in environments like the UNIX™ computer operating system.[36] This initiative brings commonality, eliminates redundancy and provides flexibility to customize for the particular environment.[37] Unfortunately this means that all users will be exposed to the threats and vulnerabilities this systems could have.

Computer Networks vulnerabilities are very well known.[38] The threat ranges from the common independent hackers to foreign nations sponsored activities. An example of this is the French Intelligence Service sponsored hacker bulletin board.[39] These Internet sites provide a wide array of freely available attack tools that can be obtained by anybody with access to the information superhighway.

Figure 4-6

The threat to JSF and the ATF continues to become more diverse as more nations continue to expand their access to information technology. The Information Systems Security (INFOSEC) technology that the government needs to protect these assets is not always readily available in commercial off-the-shelf (COTS) products. To add to the problem, INFOSEC is still seen today in many acquisition programs as an add-on function. If it is fully integrated into the engineering process, systems security posture will become more robust. Many COTS products, for example computer operating systems like Windows NT™ posses millions of lines of software code that make it extremely difficult to analyze and identify potential weaknesses. Even when trap doors or malicious code is purposely inserted, security professionals cannot find it, even when told it exists and how it works.[40] This has enormous implications to our defense. Many of the US Defense contractors utilize computer systems based on these commercial products. Their networks, which are used to develop software code for our weapons like JSF and ATF are equally vulnerable. It is plausible that an enemy could attempt to use an attack on a contractor system as a springboard to attack the ATF or JSF. To exacerbate this problem, we know that foreign intelligence services like the French General Directorate of External Security (DGSE) targets US economic and proprietary data since at least 1964.[41] The DGSE is reported to have targeted Loral Space Systems, Hughes Aircraft, and Lockheed-Martin Space Division.[42] This is especially alarming because two of the companies reportedly targeted by France, Hughes Aircraft and Lockheed are contractors in the ATF program. Lockheed-Martin is also a competitor in the CDP of the JSF program.

Information attacks on the US information infrastructure, specifically the DoD are well known.[43] As more and more nations join the GII the risks as well as the foreigners level of sophistication will continue to increase. Our information based systems like the ATF and JSF could be vulnerable in many ways but particularly because they rely in communications to unify decentralized sensor architectures when combined with other external resources. Here again, the paradigm of enhanced capability while at the same time increasing the vulnerability.

5. Conclusion

Strategy connects ends and means; it is the blueprint that shows us how resources, or means, will be employed to accomplish our ends. The ATF and JSF will play a vital role in our National Military Strategy. Although IW is not clearly understood by many and it is not consistently defined across DoD[44] it represents an opportunity and a challenge to both of these programs. It is essential the we address the IW issues as they pertain to JSF and the ATF during their development. This is imperative to their successful employment in future conflict. The DoD as a whole has recognized this issue and started to coordinate and allocate resources to address it.[45] The services have followed with the establishment of dedicated organizations towards IW.[46]

Unfortunately, it seems that in these early stages much work remains to be done towards the attainment of a unified information superiority strategy for our nation. This seems to be reflected by the different perception of what IW is among DoD. It is a complex problem that transcends the boundaries of our military as recognized by the Air Force.[47] We still have time to build a strong and flexible infrastructure that can sustain IW attacks. Making INFOSEC a fully integrated effort in our weapon systems acquisition is a necessary immediate step towards more robust weapon systems. With 47% of the world computers, 60% of the worldwide Internet resources and the most advanced global telecommunication systems we are the most dependent nation on information systems for our survival.[48]

As other countries join the global digital universe they will seek to exploit these information systems in asymmetric ways because it will be the only way the could engage the world remaining superpower. They have the most to win and we stand the most to loose. Developing a coherent and comprehensive strategy to integrate INFOSEC in DoD and Defense Contractors is necessary. This strategy should include, National Information Systems resources as well as allies and coalition friends systems. This is the best long term approach to maintain the future viability of these weapon systems.

Notes

1. National Security Council, A National Strategy For A New Century, (May 1994), 4.

2. William J. Clinton, National Security Strategy, (1997).

3. Chairman Joint Chiefs of Staff, National Military Strategy, (May 1997).

4. Chairman Joint Chief of Staff, National Military Strategy, (May 1997).

5. http://www.afa.org/f-22b.html. (14 April 1998).

6. http://www.jast.mil/assets/duplicated/pubrelbrief.pdf. (14 April 1998).

7. http://www.afa.org/f-22b.html. (14 April 1998).

8. Ibid.

9. Ibid.

10. Ibid

11. Secretary of the Air Force for Acquisition (SAF/AQ), F-22 Air Dominance Video, The Pentagon, (1997).

12. COMSEC is an acronym for Communications Security. http://csrc.ncsl.nist.gov/secpubs/nstiss.glo. (14 April 1998).

13. http://www.afa.org/f-22b.html. (14 April 1998).

14. DoDD 5000 series.

15. Office of The Undersecretary of Defense for Acquisition and Technology. Report of the Defense Science Board (DSB) Task Force on IW (Defense), (25 November 1996). Washington, D.C., 38.

16. http://www.boeing.com/defense-space/military/jsf/jsf.htm. (14 April 1998).

17. National Security Council, A New Strategy for a New Century, (May, 1997).

18. http://www.jast.mil/html/jsfwhitepaper.htm. (2 April 1998).

19. Keith V. Peifer, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, Air Force Institute of Technology, (December 1997). 47.

20. Carl Von Clausewitz, On War, ed. and trans., Michael Howard and Peter Paret. Princetown University Press, 1976, Book 6, Chapter 6, 372-376.

21. http://www.jast.mil/assets/duplicated/pubrelbrief.pdf. (14 April 1998).

22. Joint Chiefs of Staff, Joint Vision 2010, (1997).

23. Joint Chiefs of Staff, National Military Strategy, (1997).

24. DoD Directive 5000.1.

25. US Government Accounting Office, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" (GAO/AIMD-96-84), (May 1996), 15.

26. Keith V. Peifer, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, Air Force Institute of Technology, (December 1997), 1.

27. Actions taken to affect adversary information and information systems while defending one's information systems, DoDD 3600.1.

28. Ibid.

29. DoD, INFOWAR Basics CD, V.1, (1997).

30. Keith V. Peifer, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, Air Force Institute of Technology, (December 1997), 67.

31. Lawrence G. Downs, Jr., Digital Data Warfare: Using Malicious Code as a Weapon, Research Paper, Air War College, Maxwell AFB, (April 1995).

32. Wyatt C. Cook, Information Warfare: A New Dimension in the Application of Air and Space Power, Research Paper, Air War College, Maxwell AFB, (1994).

33. Dept. of the Army Field Manual 100-6, Information Operations, (August 1996), 1-6.

34. Defense Science Board Report, Report of the DSB Task Force on Information Warfare (Defense), Office of the Undersecretary of Defense for Acquisition and Technology, (November 1996).

35. Dawn Hartley, Shared Data Briefing, AFCEA Briefing. http://spider.osfl.disa.mil/dii/brief/AFCEA_brief/afcea_brief.html. (2 April 1997).

36. Ibid.

37. Ibid.

38. Defense Science Board Report, Report of the DSB Task Force on Information Warfare (Defense), Office of the Undersecretary of Defense for Acquisition and Technology, (November 1996).

39. Ibid.

40. Donald L. Brinkley and Roger R. Schell. "What Is There to Worry About? An Introduction to the Computer Security Problem," Information Security: An Integrated Collection of Essays (Los Alamitos, CA: IEEE Computer Society Press, 1995), 32-33.

41. U.S., Intelligence Threat Handbook, 3-8

42. "Telecommunications, Satellites Said to be Targeted for Espionage by France," Common Carrier Week, May 17, 1997, as reported in U.S., Intelligence Threat Handbook, 5-6

43. Defense Science Board Report, Report of the DSB Task Force on Information Warfare (Defense), Office of the Undersecretary of Defense for Acquisition and Technology, (November 1996).

44. Keith V. Peifer, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, Air Force Institute of Technology, (December 1997), 1.

45. Defense Science Board Report, Report of the DSB Task Force on Information Warfare (Defense), Office of the Undersecretary of Defense for Acquisition and Technology, (November 1996).

46. DoD, INFOWAR Basics CD, V.1, (1997).

47. Keith V. Peifer, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy, Air Force Institute of Technology, (December 1997), 67.

48. Kenneth A. Minahan, Lieutenant General, USAF, Director, National Security Agency, Public Speech, Columbia Hilton, Columbia, MD, (3 April 1997).