USAWC STRATEGY RESEARCH PROJECT

THE HUMAN DIMENSION OF NETWORK SECURITY

by

Lieutenant Colonel Dennis A. O'Brien
United States Army

Professor Stephen D. Biddle
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **03 MAY 2004**	2. REPORT TYPE	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **The Human Dimension of Network Security**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Dennis O'Brien**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES **35**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

ABSTRACT

AUTHOR: LTC Dennis A. O’Brien

TITLE: THE HUMAN DIMENSION OF NETWORK SECURITY

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 35 CLASSIFICATION: Unclassified

The transformation of the U.S. military relies heavily on new technology to wage standoff wars with limited casualties. However, network centric warfare is susceptible to numerous risks and may not be safe enough to win wars alone. This paper will examine the safety of DOD networks and the implications it has on our military forces. Specifically, it will address the human dimension of network security and vulnerabilities resulting from human error, insider threats, and deliberate hacking.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

THE HUMAN DIMENSION OF NETWORK SECURITY

> “Well-coordinated attacks by fewer than 30 computer virtuosos…with a budget of less than $10 million, could bring the United States to its knees.”
>
> —Center for Strategic and International Studies

The transformation of the US military relies on new technology and lethal targeting to wage rapid, standoff wars with limited casualties. Our doctrine and force structure is built around network operations, advances in information processing, and expectations of network performance. Precision technology has led our politicians to use the information age to guide our strategic policy decisions and minimize exposure of American troops.[1] Not surprisingly, spurred by advances in Information Technology (IT), two of Secretary of Defense Rumsfeld’s six Transformation goals are to, “Protect information networks,” and, “Use information technology to link forces to fight jointly.”[2] Additionally, “Leveraging and enabling interdependent Network-Centric warfare” is one of the Army Chief of Staff’s focused areas.[3]

Network-centric warfare has a direct impact on our military’s force structure. The Department of Defense’s (DOD’s) *Military Transformation: A Strategic Approach* discusses globalization of communications and its affect on US strategy and planning. It states that, “Transformation is necessary to ensure that U.S. forces continue to operate from a position of overwhelming military advantage…We cannot afford to react to threats slowly or have large forces tied down for lengthy periods.”[4] It adds that DOD must “move from an approach based on geographically contiguous massing of forces to one based on achieving effects.”[5] Networking provides greater situational awareness and is a key enabler of DOD’s transformation.

However, DOD networks remain susceptible to attacks caused by human error, insider threats, espionage, and deliberate hacking, potentially creating a tremendous loss of information security. Despite DOD’s best efforts, malicious activity continues to climb. Since the US military is so heavily dependent on networked information, our opponents know that both the data and connectivity are a valuable target. The military’s network operations and information processing capability may become our center of gravity and the focus of an adversary’s efforts.[6] The incentive to penetrate the network, followed by intercepting, contaminating, stealing, or even destroying data will be enormous.[7] This in turn creates problems for weapons systems depending on computers for their performance, or commanders depending on computers to manage information on today’s complicated battlefield.[8] Although DOD can defeat hackers most of the time, most of the time is not good enough when the lives of American Soldiers are at stake. There will always be problems with our networks and the associated level of risk could result in the loss of American lives.

This paper will provide a background on the reduction in the military's force structure over the past two decades, followed by a description of the Global Information Grid (GIG) and the advantages of network-centric warfare. It will then focus on human vulnerabilities and their impact on DOD networks. This argument will be substantiated by describing cryptography and the access/security tradeoff, giving the example of the German Enigma cipher, and by providing evidence on personnel reliability, insider threats, hacking, and other forms of non-cooperative access. It will also address how attacks on our critical infrastructure impact the GIG. Finally, this paper will offer recommendations to confront these challenges.

BACKGROUND

With the end of the Cold War, downsizing the US military was inevitable. In the past two decades, the US Army downsized from 18 Active Divisions and 781,000 soldiers to 10 Active Divisions and 480,000 soldiers. Much of the reason was economic; a smaller force would save money. Another reason, however, was the military's ability to leverage the advantages of the information age, including cyber warfare and satellite links. These advances in IT, combined with surveillance and precision weapons technologies, have permitted a radically new way in which we project power, reducing manpower requirements and reliance on industrial-age military forces.[9] General Schoomaker has now ordered division commanders to explore ways of reorganizing their units into modular, capabilities-based ground forces without adding more troops or equipment.[10] Rather than increasing the Army's end strength, he contends that better information will allow smaller forces to be used more effectively.

IT is now inherent in our doctrine. Several documents explain how the military will operate in the information age. Among them are the Chairman of the Joint Chiefs of Staff's *Joint Vision 2020* and DOD's *Joint Publication 3-13, Joint Doctrine for Information Operations* . *Joint Vision 2020* addresses the transformation of our military and full spectrum dominance. In order to attain these goals, the military must steadily infuse new technology and modernize. *Joint Publication 3-13* defines Information Operations (IO) as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[11] This publication also recognizes the role of defensive IO in protecting our networks. Full dimensional protection exists when the joint force can decisively achieve its mission with an acceptable degree of risk in both the physical and information domains.[12]

THE GLOBAL INFORMATION GRID AND THE ADVANTAGES OF NETWORK-CENTRIC WARFARE

The demand for a GIG was driven by concerns regarding the integration of automated information systems and the need for information and decision superiority expressed in *Joint Vision 2020.* The GIG is defined as a "Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."[13] In layman's terms, it may be compared to the World Wide Web, as it is used to collect and disseminate information. But the GIG is much more than that. It is comprised of both owned and leased communications, computing systems, and other services required to achieve information superiority. It includes DOD's Classified Network (SIPRNet), Unclassified Network (NIPRNet), 1,500 bases, posts, and stations, 100,000 Local Area Networks (LANs), and 250-500 million World Wide Web users. The Defense Information Systems Agency (DISA) coordinates the GIG's long haul connectivity for DOD and supports 40 million calls and 2,000 video conference monthly for joint task forces worldwide and policy makers from the National Command Authority to the shooter. The GIG is a "system of systems" connecting reconnaissance satellites, fusion centers, weapons platforms, commanders, and soldiers in the field, allowing the military to locate and engage with speed and efficiency while jeopardizing the lives of fewer soldiers.[14]

The GIG is essential for network-centric warfare. It plays a pivotal role in the military's transformation and ultimately in winning wars. With enhancements in C4ISR, (command, control, communications, computers, intelligence, surveillance, and reconnaissance), data concerning targets, movement of forces, and levels of equipment and supplies is collected, processed, stored, and displayed rapidly and seamlessly at different locations and levels around the globe.[15] It is argued that the GIG improves the warfighting capability of our forces by significantly reducing uncertainty, allowing collaboration for joint and asynchronous operations, and enabling the commander to achieve information superiority. The GIG has enabled the military to become lighter, faster, and more lethal.[16]

During OPERATION IRAQI FREEDOM (OIF), perhaps the first war of the information age, the fog of war was lifted to a much greater extent than in previous campaigns, as megabytes of real-time data and imagery flowed back and forth between the front lines and decision makers in remote command centers. Dramatic advances in technology provided greater fidelity, vastly improving the agility and interoperability of our units.[17] Three brigades of the 3rd Infantry Division were able to monitor each other's activity enroute to Baghdad, despite being stretched out over 300 miles.[18] General Franks, the Commander of Central Command during OIF, stated that, "Real-time communications and a common operating picture gave battlefield commanders for the first time information about the precise location and status of their troops."[19] He added that the most important lesson learned from that operation is that, "networked forces rule the battlefield."[20]

HUMAN VULNERABILITIES AND THEIR IMPACT ON DOD NETWORKS

Access to the GIG can be a great advantage yet a great risk. In order to achieve a shared sense of battlespace, individuals must have access to information and be able to connect to the network in a variety of ways. So too can the hacker. As a result of global connectivity, "a risk to one is a risk to all."[21] As the world's sole superpower, and with the global war on terrorism in full swing, nontraditional adversaries, such as the hacker, vandal, criminal, or terrorist, are of particular concern in the information domain. Since our enemies cannot compete with us on the conventional battlefield, our computing systems create a number of vulnerable fronts. The penetration of one point of defense may create havoc throughout the network as information security is compromised and data is intercepted, contaminated, or even destroyed leading to significant command and control problems.[22]

CRYPTOGRAPHY AND THE ACCESS/SECURITY TRADEOFF

The strongest tool for controlling most kinds of security threats is cryptography. Cryptography, or secret writing, uses higher mathematics, computational complexity, and probability and statistics to disguise data so that it cannot be read, modified, or fabricated easily. Although cryptography is the best defensive measure for network security, even perfect cryptography is not sufficient, as it requires humans to avoid sloppy network behavior and not to get turned or captured. Another important issue is the time it takes to decipher a message so that the scrambling and unscrambling do not deter or delay users from completing their mission.[23] For example, a 25-character message expressed in just uppercase letters has 26^{25} possible decipherments. A computer that could perform 10^{10} operations per second would require 10^{11} years to decipher the message.[24] Without the proper code, it would take an unauthorized user several lifetimes to decipher a message, by which time the content would no longer be useful.

Theoretically, hackers can be beaten with the right cryptography, but hackers can penetrate our networks because of the dilemma between easy access and robust security, otherwise known as the access/security tradeoff.[25] In bulk encryption, each layer of security is not only expensive, but introduces a latency which decreases operational responsiveness.[26] It may take a firewall only milliseconds to decrypt a packet and analyze its content, causing little to no operational impact. However, when the firewall filters or blocks the port upon which the message has been sent, latency could be indefinite.[27] This could lead to significant consequences for military forces relying on networks and data to conduct operations. Thus, the extent of computer security ends up being a tradeoff between putting the computer to use and restricting misuse.[28]

THE ENIGMA CIPHER

An example of a captured cryptography device we have observed in history is the Enigma cipher machine. The Enigma was a mechanical cryptographic tool used by the Germans in World War II to scramble messages. It was based on revolving rotors that were wired together on a typewriter keyboard. There were so many ways to encrypt messages with the Enigma, that it would take 1,000 analysts, trying four different ways per minute, 24 hours a day, seven days a week, 1.8 billion years to test them all. The technology appeared to offer perfect information security, yet broke because of human user fallibility which enabled the Allies to crack the codes.[29]

In 1938, a Polish mechanic was employed in a factory in Eastern Germany, which was making what he judged to be secret signaling machines. After being sent back to Poland, the mechanic got in touch with a British agent in Warsaw, and was soon smuggled to Paris, where he was able to make a wooden mock-up of the machine. The British Secret Intelligence Service (SIS) quickly realized it would be essential to get a hold of an actual machine if they were to stand any chance of trying to break its code. With the help of the Polish Secret Service, the British successfully smuggled an Enigma back to England. Later in the war, other Enigmas were obtained from a shot down German aircraft and from a German Tank Signals unit. In May 1941, the Navy captured a German U boat, complete with an Enigma and chart of operating keys.[30]

The SIS was located at Bletchley Park, fifty miles north of London. At Bletchley, along with the Government Code and Cypher School, the SIS set out to break the Enigma code. By using captured Enigmas, making use of likely chatter about daily events, and guessing that the Germans would be discussing certain places or issues, the British found sections of scrambled text that could be related to cleartext. They also concentrated on Luftwaffe messages. Luftwaffe signalmen often used girlfriends' names for key settings, or would begin a second message with the same key setting as the previous message. This knowledge helped the Allies break the Enigma code and determine the Luftwaffe's plans during the Battle of Britain.[31] Intelligence gathered from Enigma significantly contributed to the Allies' victory in World War II.

PERSONNEL RELIABILITY AND THE INSIDER THREAT

The story of the Enigma cipher machine shows us that new technologies remain vulnerable to human error, often caused by complacency. Used correctly and protected properly, Enigma's code was unbreakable. But a spy gave away its existence, capture provided the equipment and codebooks, and sloppy user behavior gave British code breakers critical help. It was the people, not the technology, that undermined Enigma. Could the same thing happen today?

Even when dangerous technologies are used and lives are at stake, our unchanging fallibility remains. For example, according to the U.S. General Accounting Office, human error contributed to 75% of the most serious US military aircraft accidents in 1994 and 1995. Additionally, the Union of Concerned Scientists of ten nuclear power plants found that 80% of reported problems in nuclear power plants resulted from worker mistakes or poorly designed procedures. In November 1999, the Institute of Medicine of the U.S. National Academy of Sciences reported that medical errors cause more deaths each year in the US than AIDS or breast cancer. For all the risks involved, much of the day-to-day work of the individuals dealing with these technologies is quite boring. This leads to a monotonous working environment, a lack of vigilance, and individuals not paying close attention to the task at hand.[32] These same kinds of human errors threaten DOD networks.

DISA's Field Security Operations (FSO) Division provides Information Assurance (IA) support to DOD organizations to include the Combatant Commands. IA employs multilevel security, intrusion detection software, and other access controls to defend information and information systems, as well as measures for availability and reliability of information.[33] FSO reviews programs with the goal of raising the IA posture of DOD. Their teams have identified consistent deviations from DOD requirements in the following areas: IA documentation is often incomplete or missing, configuration management programs which protect the system while it is being designed and maintained[34] are not in place, and physical protection of the SIPRNet is marginal. Web cameras were found in secure areas capable of observing a terminal on a classified network, and foreign nationals were found in areas where the SIPRNet (a US–only network) was present. Lack of due diligence also leads to fielding new systems without consideration of security implications. For example, at least one command introduced Voice over Internet Protocol into the network environment before it was patched for virus protection.[35]

Although most DOD employees want to do a good job, 64% of the 249 unauthorized DOD intrusions reported in the first quarter of FY04 resulted from poor security practices.[36] Even though the means are available to plug holes in network security, too few individuals and organizations take advantage of them.

As we have become increasingly dependent on information systems, the overwhelming focus of attention on the vulnerability of the Nation's networks has been devoted to computer crime and security attacks from external sources, exemplified by the President's Commission on Critical Infrastructure Protection. Yet, losses due to insiders greatly outweigh those due to hackers and other external sources. According to the Computer Security Institute's *1998 Computer Crime Survey,* the average cost of a hacker penetration was $56,000, while insider attacks cost companies $2.7 million. A study conducted by the United Nations Commission on Crime and Criminal Justice, which surveyed 3,000 Virtual Address Extension sites, found that the greatest security threat came from employees or other insiders with access to computers.[37]

A significant security risk arises when the trusted insider, a dissenter or disgruntled employee, crashes the system or corrupts information with viruses. Now, an individual associated with a network can significantly damage an organization at great speed, or could bring an entire network down. These may be individuals tasked with the design, maintenance and operation of networks who hold positions of unprecedented importance and trust. Malevolence on the part of an insider can have grave consequences, and the range of perpetrators and their possible motivations is broad. In many cases, sabotage has been committed by disgruntled employees who are angry about lay-offs or transfers. Other employees may take advantage of their position for financial gain. Overall, the number of computer-related offenses committed by trusted insiders is rising rapidly each year. According to WarRoom Research's *1996 Information Systems Security Survey,* nearly 63% of the companies surveyed reported insider threats to their networks.[38]

Some experiences drawn from the civilian sector can lend perspectives on the likely scale of the insider threat to the GIG. Additionally, evidence indicates that DOD is not invulnerable to such threats. A number of cleared military service members, DOD or contractor employees commit acts of espionage each year. Between 1975 and 1999, the Defense Personnel Security Research Center reported 105 cases of espionage, including the names of former National Security Agency (NSA) staffers and Army communications personnel. These were just the individuals who were caught, suggesting a lower bound on the actual number of acts of espionage. In 1998, David Sheldon Boone, a former Army signals analyst for the NSA, was arrested for selling Top Secret documents to the Soviet Union from 1988 to 1991, including a manual describing US reconnaissance programs. In 1996, Robert Stephen Lipka, also a former NSA staff member, was arrested for committing espionage while an Army communications clerk. Between 1964 and 1967, Lipka worked in the NSA central communications room. He provided the KGB with a constant stream of highly classified reports, and is believed to have caused extensive damage to US intelligence collection activities. Lipka also may have been responsible for the loss of American lives during the Vietnam War.[39] As recently as 12 February 2004, Specialist Ryan G. Anderson, a member of the Washington State National Guard, was arrested after offering his services to Al Qaeda via the Internet.[40]

Although traitors have always existed, until recently the amount of damage an individual could inflict was marginal. IT greatly increases opportunities for espionage and the damage that can be caused by a single traitor. Since the preponderance of battlefield message traffic is carried over the SIPRNet, these cases also demonstrate the damage that insiders can inflict on the GIG during combat, and the potential loss of lives that could result from infiltrating DOD networks or tainting data.

HACKING AND OTHER FORMS OF NON-COOPERATIVE ACCESS

> “Digi criminals are already having a great time...the outlook for protection is bleak.”
>
> —Arjen Lenstra

A hacker is defined as, “a person who “hacks” away at a programmable system (i.e., computer system and applications software) until it works. In contemporary lingo, a person who breaks into computer systems, usually over the Internet.”(sic)[41]

A hacker can initiate an attack using commercial off-the-shelf products, or even hacker tools from the Internet. He can directly attack DOD unclassified systems or strike indirectly by conducting a strategic attack on power grids or other public utilities.[42] Another threat to the network is the distributed denial of service attack, in which a web server is bombarded with huge amounts of data from many different machines with the intention of bringing the server down. Malicious code, in the form of a Trojan horse (a program that overtly does one thing yet covertly does another), a virus (a Trojan horse that spreads an infection from one computer to another), or a worm (a program that spreads copies of itself as a stand-alone program through a network),[43] can destroy or impede systems configurations or routines.[44]

The DOD Computer Emergency Response Team (CERT) is DOD’s technical Computer Network Defense Response center. Their mission is to protect DOD Networks and computer infrastructure. They maintain global situational awareness of the GIG through sensors at 21

Internet gateways and 625 enclaves, intelligence and hacker source research, and response center input. DOD CERT routinely monitors and blocks viruses, such as KAK and Loveletter in 2000, and malicious worms, such as the Chinese Hacker War and Code Red in 2001 .[45]

DOD CERT security indicators show that the GIG is under constant attack. The following illustrations reflect malicious activity and attacks on information networks.

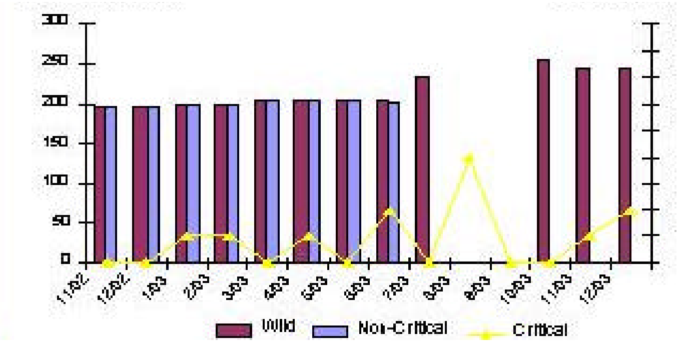

FIGURE 1 – INTERNET VIRUS GROWTH PER MONTH

Figure 1 shows the level and severity of malicious code across the Internet. It depicts the total number of viruses compared to the number of critical or dangerous viruses as determined by DOD CERT. A virus is listed as “Wild” by WildList.org when it is reported by two sources. DOD CERT reports that the number of critical is increasing, the impact of each critical is increasing,[46] and the speed of propagation of malicious code is increasing,[47] raising the vulnerability of DOD networks.

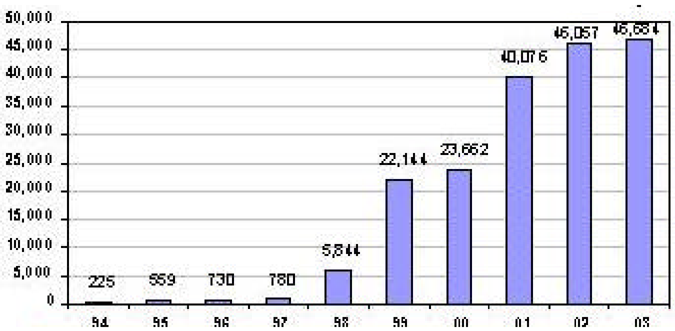

FIGURE 2 – DETECTED EVENTS ON THE NIPRNET

Figure 2 shows the overall number of detected events on the NIPRNet. In the past ten years, there has been a constant growth in events reported by DOD CERT. These include root and user level compromises, denial of service attacks, and compromises resulting from poor security practices. Although this increase can be attributed in part to better sensors and reporting procedures, it may also reflect a significant increase in malicious activity. [48]

DOD CERT uses Internet Protocol (IP) addresses to indicate scanning source locations. On 6 April 2002, an IP address from the St. Petersburg, Russia Public Internet Center scanned over 50,000 DOD hosts, and from 10 February to 10 March 2002, the NEXCOM Tron in Yekaterinburg, Russia scanned over two million DOD hosts. These are indicators of threats from around the world searching for potential vulnerabilities to DOD networks.[49] Recent statistics from January 2004 indicate that the top three source countries for unauthorized probes are the US, Korea, and China. However, this may not represent the actual source, as an attacker may hop from country to country, nor does it imply government involvement.[50]

ATTACKING OUR CRITICAL INFRASTRUCTURE

The GIG includes systems DOD neither owns nor controls. Between 80 and 90 percent of critical infrastructure, including telecommunications, is either owned or operated by private firms, thereby making it hard for DOD to control. Yet similar human vulnerabilities occur in non-DOD networks. While winning the global war on terror and defending the homeland remain the primary missions of the military, national systems and corporations are having difficulty keeping hackers out.

Numerous departments and agencies, such as the CIA, the Departments of Defense, Justice, Treasury, and Commerce have a stake in IO.[51] As they become increasingly automated and dependent on networks, a huge vulnerability arises. This includes susceptibility to cyber attack. Publicity of attacks on these departments is increasing, demonstrating that while we are the most technologically advanced nation, we are also the most technologically dependent.[52] As recently as September 2003, a computer virus crippled the State Department's Consular Lookout and Support System, known as CLASS. CLASS contains over 12.8 million records from the FBI and the State Department, including the names of 78,000 suspected terrorists.[53] The government also confirmed that disruptions occurred in two important internal systems at Lake Erie's Davis-Besse nuclear power plant in January 2003 resulting from the Slammer infection.[54] Corporations are also experiencing compromises to information security following cyber-attacks. Riptech Inc., a security firm in Alexandria, Virginia, reported that Internet attacks against private organizations jumped 28% during the first six months of 2002.

Most attacks targeted technology, finance, and power companies.[55] A 1996 FBI survey reported that $4.5 billion was lost to businesses who had their networks compromised. Forty-two percent of all businesses experienced attacks, and of these, 58% cited competitors as the likely attacker.[56]

Some argue that the vulnerabilities to our interlinked infrastructure are blown out of proportion. George Smith, editor of *The Crypt Newsletter* and author of *The Virus Creation Labs: A Journey into the Underground*, suggests that an "Electronic Pearl Harbor" is unlikely. Smith notes that the private sector will not disclose much information about potential vulnerabilities, often because they are embarrassed about compromises to their networks and the potential loss of customers. Many of the individuals who suggest a problem exists are in the business of selling security devices and are not in a position to serve as objective sources of information. Even if a hacker can invade a system, it would be difficult for him to alter a database or issue reports without inside knowledge. Additionally, hoaxes about computer viruses are often propagated more than the real thing, inflating the numbers and adding confusion over what is real and what is not. In other words, it is hard to measure success or even the extent of the problem.[57] However, Smith does not address the human dimension of network security. The insider threat, for example, is a significant concern which cannot be assumed away.

Others predict more alarming conclusions. Newt Gingrich, former Speaker of the House and member of the Commission on National Security/21st Century, writes that the United States faces serious threats from Internet-borne weapons. He states that our adversaries are developing methods for disrupting our quality of life, from infiltrating our financial systems to breaking down communications systems and initiating electrical blackouts. Such an attack could result in serious loss of life and widespread damage to our infrastructure, potentially destabilizing the nation. Gingrich's commission concluded that the relative ease of hacking increases the threat of cyber attacks, in comparison to the difficulty of developing nuclear, chemical, or biological weapons.[58] A recent survey conducted by Pew Internet & American Life Project, showed that many Americans fear a terrorist cyber attack. 50 percent of adults felt our national infrastructure was vulnerable to terrorist hackers. These fears are backed by technology experts. Paul Henry, vice president of CyberGuard Corp concluded, "I think there is an 80% probability we could see an attack in the next two years."[59]

RECOMMENDATIONS

> "Information Networks must be controlled, protected, and managed as effectively as weapons systems."
>
> —LtGen Harry D. Raduege, DISA Director

Given the critical role played by the GIG in today's warfighting environment, reliable protection of data and the defense of our networks are essential. DOD is in the process of implementing several IA GIG initiatives to counter the threats and vulnerabilities to our networks. Many of these changes are long overdue and the possible IA implications associated with these emerging security technologies are significant. An enormous effort remains to be done at the organizational and individual level.

HEIGHTENED SECURITY AWARENESS AND INSIDER PROTECTION

High-tech network equipment requires high quality training for users who must apply the concepts of IA to protect DOD networks and stay ahead of our adversaries.[60] Network security professionals must be certified on security standards and procedures. Information must be recompartmentalized so that access control of the private differs from the general. Another solution is to have fewer access points and restrictions for certain individuals, or have access based on rank, position, or nationality.[61] Although all of these measures are being done now and the guidance is there, people still make mistakes.[62] FSO continues to find differing levels of completeness in organizations' training and certification requirements, and annual refresher training is rare.[63]

The first line of defense for network users is implementation of access control measures such as secure passwords. Another access control measure is the Fortezza card, a common access card which secures sensitive but unclassified data for transmission over unsecured networks. Passwords should be at least 8 characters long, alphanumeric, and changed regularly to prevent them from being machine–guessed. DOD has an 8 character password standard, although FSO has found organizations in violation of DOD's policy.[64] Use of software products that check passwords for compliance is growing but is not universal.[65] Nor is the use of Fortezza cards.

The installation of a firewall will allow only selected gateways to have access to the outside world. Other methods for improving computer network defense include ports and protocols configuration control to block selected ports, anti-virus software, and intrusion detection systems to cope with malicious inputs.[66] DOD has implemented these measures, although the use of additional firewalls beyond the enclave perimeter and the use of personal firewalls on traveling laptops are rare.[67]

Network security is not just an individual responsibility. Military leaders and managers in both government and the private sector must ensure users complete IA training before being given access to a system, and then receive annual refresher training to keep pace with technology upgrades and the discovery of new vulnerabilities. Leaders must implement and enforce consistent policies and procedures in computer security with significant consequences for offenders. Commanders must be held responsible for a lack of security in their organization. Although most people in the military, the government, and corporate America work with information systems, computer security is still practiced half-heartedly. [68]

Additionally, commanders must make an operational risk assessment, striking a balance between all net centric (100% accessibility to our networks) and no net centric (0% accessibility). Reducing the connectivity of the network to reduce vulnerabilities also decreases the power of the network. On the other hand, increasing network security will restrict access and also increase response time, arguably decreasing operational capability. If the commander gives up connectivity to increase security, he is essentially taking steps backwards regarding network-centric warfare. For example, installing a firewall to increase security reduces connectivity because less packets will be allowed to pass through. Password protection and Fortezza cards also reduce connectivity because users will forget their passwords or lose their Fortezza cards. Ultimately, we decide how many voluntary reductions in connectivity we want in order to increase security. This is the access/security tradeoff.

Many of the same measures needed to heighten security awareness for users should be used to protect DOD networks from insiders. In addition to using access control measures such as secure passwords and Fortezza Cards, another helpful but inevitably partial improvement might be for commanders to ensure only selected people have access. For example, more and more individuals are using the SIPRNet, increasing the probability that someone will be negligent or commit espionage. Arguably, such an individual with access to the SIPRNet could cause significant damage to US military operations possibly resulting in the loss of American lives. As the SIPRNet grows, perimeter security must be built internally within its enclaves to compartmentalize information and access. Physical measures, such as access badges and secure doors should also be used as aggressively as possible to limit access.

FSO has also found that configuration management programs do not exist in most organizations.[69] Software initiatives will potentially help with configuration management, thereby improving DOD's IA posture.[70] MIT responded to insider threats by introducing Kerberos, a network authentication protocol that protects passwords and other sensitive information through the use of cryptography. Kerberos uses Data Encryption Standard (DES) to encrypt, and relies on a central authentication server for security.[71] Interviews with experts indicate that Kerberos is a tremendous security tool with an excellent reputation.

Human vulnerabilities cannot be solved with technological solutions alone. Without examining the insider problem and developing new methods of insider risk management, our critical information systems will remain vulnerable to espionage or sabotage by insiders. Leaders must conduct initial pre-employment screening of employees, to include collecting trait information and conducting a criminal records check. They must establish rules of conduct to guide employees on right and wrong behavior and give supervisors the recourse to punish rule violations. Leaders must ensure that systems administrators revoke access privileges of selected employees prior to lay-off announcements. Ultimately, the highest mitigating factor that reduces the likelihood of an insider attack is intervention by supervisors, co-workers, family or friends. Intervention might lead to counseling or even medical assistance, and may prevent network disasters from occurring.[72] But presumably, all these measures were in use for the espionage cases cited earlier, yet they failed.

TRANSFORMATIONAL GIG INITIATIVES AND DOCTRINAL CHANGES

Numerous transformational GIG initiatives are underway to avert network vulnerabilities and make it easier for users to do the right thing. These include Internet Protocol Version 6, a network layer protocol which will improve end-to-end security and quality of service. The DOD Cryptographic Modernization Initiative is leveraging new technology, such as secure voice and key management, to provide IA solutions to protect the GIG and the critical information contained therein.[73]

Still, it is difficult to measure success and determine if these actions are sufficient. Even if hacking as a whole is reduced, one hacker can still cause tremendous damage. And we often do not know when penetration occurs . This has profound consequences to our Armed Forces. During World War II, Enigma provided Churchill advance warning of a German air strike on Coventry, yet he chose to sacrifice lives rather than reveal to Hitler that the Allies had cracked the unbreakable Enigma code.[74] For much of the war, the Germans failed to realize Enigma had been compromised. Just as the Allies had knowledge of Enigma messages in World War II, today an adversary could have access to GIG message traffic without our knowledge. Although NIPRNet traffic is more routine than SIPRNet traffic, infiltration of the NIPRNet in the form of a denial of service attack or malicious code can still damage the GIG, and user trust and confidence in DOD networks and data. Even redundant lines of communication cannot help if data has been tainted. For example, if a commander uses SIPRNet traffic for targeting purposes, he expects the data to be timely, accurate, and consistent. If his data has been corrupted, it can affect his situational awareness and put his soldiers at risk.

This also has an impact on a military in transformation, which is in the process of reorganizing into even smaller modular units. Smaller conventional forces have less inherent firepower making them more vulnerable to attack. Smaller units also have less human knowledge power. This creates additional challenges for units relying on technology and information processing to conduct operations. For example, when networks and computers go down, Artillery units will have more difficulty conducting fire missions.[75] Without the global positioning system, units will have more difficulty maneuvering. Our Armed Forces must be prepared for network failures and train in these conditions. They must understand the Commander's Intent and have the initiative to carry on with their mission when networks go down.

Another limitation on exploiting technology is the parochial organization system found in the military, which tends to adapt slowly. [76] Yet transformation must be accompanied by changes in doctrine, culture, and behavior. Computer network operations is a new, sensitive, and complex mission with unique challenges. The changing nature of warfare, caused by both the end of the Cold War and advances in technology, brings with it new fields of expertise for military professionals.[77] The Army must invest in her employees to adapt to the IO environment, and develop a strategy for IO to support force development. However, training and educating personnel on IO often takes a back seat to operational requirements. Even today, many senior commanders are unable to grasp the full utility of IO. [78]

Interviews with experts have also revealed that despite DOD's transformational GIG initiatives, tools such as firewalls are often pushed out after the fact, decreasing their effectiveness in protecting DOD networks. Although the threats to the GIG are growing, network support staffs are being downsized.[79] In most organizations, manpower and funding to implement IA is resourced on an ad hoc basis. Including IA in the command's Planning, Programming, and Budgeting System (PPBS) is rare.[80]

Conceivably, a lone fanatic or sophisticated adversary can create the cyberspace equivalent of a 9/11 sneak attack, paralyzing our communications systems and the GIG. The reality that human vulnerabilities can threaten our critical infrastructure creates a new national defense problem and makes our traditional means of deterrence unworkable. Deterrence works if there is a group or country that can be retaliated against for unacceptable behavior. However, if the opponent is a lone individual, then conventional military strikes are not an option. We need a new public-private partnership to confront the vulnerabilities to our networks.[81] Organizations, such as the Department of Commerce's Critical Infrastructure Assurance Office and the FBI's National Infrastructure Protection Center, were established to educate civilian industry and improve critical infrastructure protection. Unfortunately, cooperation between the government and the civil sector is lacking, and progress to protect our critical infrastructure is slower than desired.[82]

These are all useful and important steps. At the margin, they will improve security. But nothing can repeal human nature. The most technically secure network in the world can still be undone by an unreliable insider, and we have never been able to guarantee 100% personnel reliability. There will always be the occasional spy; some operators will always be careless or tired or overworked leading to compromises in DOD networks.

CONCLUSION

Growing confidence in advancing technology has made both politicians and the public alike believe that extreme technological superiority is the answer to the problems of war, and that our downsized military can accomplish any mission with high-tech weaponry and network-centric warfare. However, evidence shows that the GIG is fragile. Threats to DOD networks are increasing with the number of attacks and the speed of propagation of malicious code. Furthermore, DOD CERT statistics and interviews with experts indicate that the determined hacker has successfully gotten into our networks, particularly the NIPRNet. Human behavior being what it is, the NIPRNet and even the SIPRNet will remain vulnerable. If the SIPRNet is better protected than the NIPRNet, it is a difference of degree, not kind.

This has serious implications to our military's force structure. Because of their reduced manpower, smaller conventional forces have less inherent firepower and knowledge power, and are therefore more vulnerable to attack, particularly if the networks and data they are relying on have been compromised. What if a small unit from OIF relied on a SIPRNet terminal, Blue Force Tracking, or a similar device connected to the GIG to conduct combat operations? What if another terminal connected to the GIG was turned over by an insider, was captured by the enemy (like the Enigma), or the data was intercepted or corrupted by an Iraqi hacker? Without perfect data, the unit's situational awareness would become distorted, leading to possible command and control problems or even the loss of American lives.

Although measures such as DOD's transformational GIG initiatives are being implemented to mitigate threats to DOD networks, despite our best efforts, the risks will never be completely eliminated. Human vulnerabilities in the information domain are an unsolvable Achilles' heel. Our senior leaders must understand that DOD networks will never be 100% secure. Perhaps we should reconsider transformation initiatives relating to force structure in light of a more systematic analysis of all the threats to our information systems, to include the human threat. There are only so many approaches to network security. Human vulnerabilities underlie them all.

WORD COUNT=6533

ENDNOTES

[1] Richard J. Harknett and the JCISS Study Group, “The Risks of a Networked Military,” *Orbis* Volume 44, Number 1 (Winter 2000): 129.

[2] Defense Information Systems Agency, “Command Brief,” briefing slides, Arlington, VA, Headquarters DISA, 5 March 2002.

[3] Department of the Army, *An Army at War Relevant and Ready*, (Washington, D.C.: U.S. Department of the Army, 23 October 2003), 4.

[4] Department of Defense, *Military Transformation: A Strategic Approach* (Washington, D.C.: U.S. Department of Defense, Fall 2003), 12.

[5] Department of Defense, *Military Transformation: A Strategic Approach*, 32.

[6] Peter D. Feaver, “Blowback: Information Warfare and the Dynamics of Coercion,” *Security Studies* Volume 7, Number 4 (Summer 1998): 88-91.

[7] Harknett, 131.

[8] Feaver, 96.

[9] Harknett, 127-128.

[10] Nathan Hodge, “Service Chiefs Don’t Seek Boost In End Strength,” *Defense Week Daily Update*, 3 December 2003, 1.

[11] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13 (Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October 1998), vii.

[12] Joint Chiefs of Staff, *Joint Vision 2020*, (Washington, D.C.: U.S. Joint Chiefs of Staff, June 2000), 26.

[13] Joint Forces Command, *Capstone Requirements Document Global Information Grid* (Norfolk, VA: Headquarters Joint Forces Command, 28 March 2001), 1.

[14] Defense Information Systems Agency, “Command Brief.”

[15] Joint Forces Command, *Capstone Requirements Document Global Information Grid*, 4.

[16] The ideas in this paragraph are based on remarks made by a speaker participating in the Commandant’s Lecture Series.

[17] Matthew Brzezinski, “The Unmanned Army,” *ROA National Security Report* (July/August 2003): 35.

[18] Megan Scully, “Iraq War Proves Power of Net-Centric Vision,” *Defense News*, 26 January 2004, 1.

[19] Matthew French, “Franks: Net-centric tech is “heaven”,” 22 January 2004; available from http://www.fcw.com/fcw/articles/2004/0119/we-franks-01-22-04.asp; Internet; accessed 30 January 2004.

[20] French.

[21] Defense Information Systems Agency, *DOD Information Assurance Awareness*, (Arlington, VA: Headquarters DISA, September 2001), compact disk.

[22] Harknett, 131.

[23] Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing* (Upper Saddle River, NJ: Prentice Hall, 2003), 35.

[24] Pfleeger, 40.

[25] Harknett, 131.

[26] Mark Orndorff and Tom Harrison of DISA Field Security Operations, interview by author, 14 January 2004, Chambersburg, PA.

[27] Jerry Ratliff of DISA Field Security Operations, telephone interview by author, 1 March 2004.

[28] S. M. Lieu, “Computer and Network Security,” 26 April 1995, [database on-line]; available from Netsurfer Focus; accessed 12 January 2004.

[29] Pfleeger, 65.

[30] F. W. Winterbotham, *The Ultra Secret* (New York, NY: Dell Publishing Co.,1974), 26-51.

[31] Pfleeger, 65.

[32] Lloyd J. Dumas, “Betting Against Nature: Human Fallibility and Dangerous Technologies,” briefing for the Annual Meeting of the Friends Committee on National Legislation: Washington, D.C., 9 November 2001.

[33] Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Pub 3-13, III-1.

[34] Deborah Russell and G. T. Gangemi Sr., *Computer Security Basics* (Sebastopol, CA: O’Reilly & Associates, Inc., 1991), 145.

[35] Defense Information Systems Agency, *Information Assurance Support Trends Report* (Arlington, VA: Headquarters DISA, 31 December 2003), v-17.

[36] Defense Information Systems Agency, “Leading CND Security Indicators,” briefing slides, Arlington, VA, Headquarters DISA, 10 January 2004.

[37] Eric D. Shaw, Keven G. Ruby, and Jerrold M. Post, “The Insider Threat to Information Systems,” 7 September 2001; available from http://www.dss.mil/training/csg/security/Treason/Infosys.htm; Internet; accessed 27 January 2004.

[38] Shaw.

[39] Defense Personnel Security Research Center, “Recent Espionage Cases 1975-1999,” 12 February 2002; available from http://www.dss.mil/training/espionage/; Internet; accessed 12 January 2004.

[40] Michael Janofsky, “Guardsman Taken Into Custody And Examined For Qaeda Tie,” *New York Times*, 13 February 2004.

[41] Harry Newton, *Newton’s Telecom Dictionary* (New York: CMP Books, 2002), 341.

[42] Joint Chiefs of Staff, *Manual for Employing Joint Tactical Communications*, CJCSM 6231.01A (Washington, D.C.: U.S. Joint Chiefs of Staff, 23 May 1997), B-1.

[43] Pfleeger, 15, 112.

[44] Defense Information Systems Agency, *DOD Information Assurance Awareness.*

[45] Defense Information Systems Agency, “Command Brief.”

[46] Defense Information Systems Agency, “Leading CND Security Indicators.”

[47] Larry Huffman, “Information Assurance Operations: Present and Future,” *Defense Information Systems Agency Customer Connection* Volume 2, Number 2 (July 2002): 3.

[48] Defense Information Systems Agency, “Leading CND Security Indicators.”

[49] Huffman, 2.

[50] Defense Information Systems Agency, “Leading CND Security Indicators.”

[51] Feaver, 112.

[52] Joint Forces Staff College, *Joint Information Operations Planning Handbook* , (Norfolk, VA: March 2001), D-7.

[53] Ted Bridis, “Computer Virus Leaves U.S. Unable to Run Visas Checks,” *Patriot-News*, 24 September 2003, sec. A, p. 9.

[54] Ted Bridis, “NRC Warns N-plants of Internet Infections,” *Patriot-News*, 4 September 2003.

[55] Michael Barbaro, “Internet Attacks on Companies Up 28 Percent, Report Says,” *Washington Post*, 8 July 2002, sec. E, p. 5.

[56] Congress, Committee on Science, Subcommittee on Technology, *The Role of Computer Security in Protecting U.S. Infrastructures*, 6 November 1997, 4.

[57] George Smith, “An Electronic Pearl Harbor? Not Likely,” *Issues in Science and Technology Online*, Fall 1998, 1-9.

[58] Newt Gingrich, “Threats of Mass Disruption,” *Information Security Magazine*, April 2001, 1.

[59] “Poll Finds Americans Fear Cyberattack,” *Patriot-News*, 4 September 2003, sec. A, p. 2.

[60] Defense Information Systems Agency, *DOD Information Assurance Awareness.*

[61] Harknett, 132.

[62] Orndorff.

[63] Defense Information Systems Agency, *Information Assurance Support Trends Report*, 10.

[64] Defense Information Systems Agency, *Information Assurance Support Trends Report*, 14.

[65] Pfleeger, 218-219.

[66] Defense Information Systems Agency, “Command Brief.”

[67] Defense Information Systems Agency, *Information Assurance Support Trends Report*, 12.

[68] Smith, 9.

[69] Defense Information Systems Agency, *Information Assurance Support Trends Report*, 3.

[70] Defense Information Systems Agency, *Information Assurance Support Trends Report*, vi.

[71] Lieu.

[72] Shaw, 12.

[73] Department of Defense, *Joint Transformation Roadmap, Pre-Decisional Draft* (Washington, D.C.: U.S. Department of Defense, 3 November 2003), 73.

[74] Winterbotham, 94-95.

[75] Tim Rosenberg of White Wolf Consultants, interview by author, 2 March 2004, Carlisle Barracks, PA.

[76] William E. Odom, “Transforming the Military,” *Foreign Affairs* Volume 76, Number 4 (July /August 1997): 63.

[77] Don M. Snyder, “Jointness, Defense Transformation, and the Need for a New Joint Warfare Profession,” *Parameters* Volume XXXIII, Number 3 (Autumn 2003): 21.

[78] Joint Forces Staff College, D2.

[79] Orndorff.

[80] Defense Information Systems Agency, *Information Assurance Support Trends Report*, 8.

[81] Gingrich, 1-2.

[82] Joint Forces Staff College, D8-9.

BIBLIOGRAPHY

Barbaro, Michael. “Internet Attacks on Companies Up 28 Percent, Report Says.” *Washington Post*, 8 July 2002, sec. E, p. 5.

Bridis, Ted. “Computer Virus Leaves U.S. Unable to Run Visas Checks.” *Patriot-News*, 24 September 2003, sec. A, p. 9.

________. “NRC Warns N-plants of Internet Infections.” *Patriot-News*, 4 September 2003.

Brzezinski, Matthew. “The Unmanned Army.” *ROA National Security Report* (July/August 2003): 35.

Defense Information Systems Agency. “Command Brief.” Briefing slides. Arlington, VA: Headquarters DISA, 5 March 2002.

________. *DOD Information Assurance Awareness*. Arlington, VA: Headquarters DISA, September 2001. Compact disk.

________. *Information Assurance Support Trends Report.* Arlington, VA: Headquarters DISA, 31 December 2003.

________. “Leading CND Security Indicators.” Briefing slides. Arlington, VA: Headquarters DISA, 10 January 2004.

Defense Personnel Security Research Center. “Recent Espionage Cases 1975-1999.” 12 February 2002. Available from http://www.dss.mil/training/espionage/. Internet. Accessed 12 January 2004.

Dumas, Lloyd J. “Betting Against Nature: Human Fallibility and Dangerous Technologies.” Briefing for the Annual Meeting of the Friends Committee on National Legislation. Washington, D.C., 9 November 2001.

Feaver, Peter D. “Blowback: Information Warfare and the Dynamics of Coercion.” *Security Studies* Volume 7, Number 4 (Summer 1998): 88-91.

French, Matthew. “Franks: Net-centric tech is “heaven”.” 22 January 2004. Available from http://www.fcw.com/fcw/articles/2004/0119/we-franks-01-22-04.asp. Internet. Accessed 30 January 2004.

Gingrich, Newt. “Threats of Mass Disruption.” *Information Security Magazine*, April 2001, 1.

Harknett, Richard J., and the JCISS Study Group. “The Risks of a Networked Military.” *Orbis* Volume 44, Number 1 (Winter 2000): 129-133.

Hodge, Nathan. “Service Chiefs Don’t Seek Boost In End Strength.” *Defense Week Daily Update*, 3 December 2003, 1.

Huffman, Larry. “Information Assurance Operations: Present and Future.” *Defense Information Systems Agency Customer Connection* Volume 2, Number 2 (July 2002): 3.

Janofsky, Michael. “Guardsman Taken Into Custody And Examined For Qaeda Tie.” *New York Times*, 13 February 2004.

Joint Forces Command. *Capstone Requirements Document Global Information Grid.* Norfolk, VA: Headquarters Joint Forces Command, 28 March 2001.

Joint Forces Staff College. *Joint Information Operations Planning Handbook.* Norfolk, VA: March 2001.

Lenstra, Arjen. “Communication.” *Spectrum* (January 1996): 32. Quoted in James Stavridis. “The Second Revolution.” *JFQ* (Spring 1997): 10.

Lieu, S. M. “Computer and Network Security.” 26 April 1995. Database on-line. Available from Netsurfer Focus. Accessed 12 January 2004.

Newton, Harry Newton. *Newton’s Telecom Dictionary.* New York: CMP Books, 2002.

Odom, William E. “Transforming the Military.” *Foreign Affairs* Volume 76, Number 4 (July /August 1997): 63.

Orndorff, Mark, and Tom Harrison, DISA Field Security Operations. Interview by author, 14 January 2004, Chambersburg, PA.

Pfleeger, Charles P., and Shari Lawrence Pfleeger. *Security in Computing.* Upper Saddle River, NJ: Prentice Hall, 2003.

“Poll Finds Americans Fear Cyberattack.” *Patriot-News*, 4 September 2003, sec. A, p. 2.

Raduege, Harry D. Quoted in Defense Information Systems Agency. “Command Brief.” Briefing slides. Arlington, VA: Headquarters DISA, 5 March 2002.

Ratliff, Jerry, DISA Field Security Operations. Telephone interview by author, 1 March 2004.

Rosenberg, Tim, White Wolf Consultants. Interview by author, 2 March 2004, Carlisle Barracks, PA.

Russell, Deborah, and G. T. Gangemi Sr. *Computer Security Basics.* Sebastopol, CA: O’Reilly & Associates, Inc., 1991.

Scully, Megan. “Iraq War Proves Power of Net-Centric Vision.” *Defense News*, 26 January 2004, 1.

Shaw, Eric D., Keven G. Ruby, and Jerrold M. Post. “The Insider Threat to Information Systems.” 7 September 2001. Available from http://www.dss.mil/training/csg/security /Treason/Infosys.htm. Internet. Accessed 27 January 2004.

Smith, George. “An Electronic Pearl Harbor? Not Likely.” *Issues in Science and Technology Online*, Fall 1998, 1-9.

Snyder, Don M. “Jointness, Defense Transformation, and the Need for a New Joint Warfare Profession.” *Parameters* Volume XXXIII, Number 3 (Autumn 2003): 21.

Stavridis, James. “The Second Revolution.” *JFQ* (Spring 1997): 10.

U.S. Congress. Committee on Science. Subcommittee on Technology. *The Role of Computer Security in Protecting U.S. Infrastructures.* 6 November 1997.

U.S. Department of Defense. *Joint Transformation Roadmap, Pre-Decisional Draft.* Washington, D.C.: U.S. Department of Defense, 3 November 2003.

________. *Military Transformation: A Strategic Approach.* Washington, D.C.: U.S. Department of Defense, Fall 2003.

U.S. Department of the Army. *An Army at War Relevant and Ready.* Washington, D.C.: U.S. Department of the Army, 23 October 2003.

U.S. Joint Chiefs of Staff. *Joint Doctrine for Information Operations.* Joint Pub 3-13. Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October 1998.

________. *Joint Vision 2020.* Washington, D.C.: U.S. Joint Chiefs of Staff, June 2000.

________. *Manual for Employing Joint Tactical Communications*, CJCSM 6231.01A. Washington, D.C.: U.S. Joint Chiefs of Staff, 23 May 1997.

Winterbotham, F. W. *The Ultra Secret.* New York, NY: Dell Publishing Co., 1974.