REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: Office of the Provost	
6. Office Symbol: NWC Seminar 12	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Protecting Our Critical Information Technology Systems	
9. Personal Authors: BABETTE M. LENFANT, Lt Col, USAF	
10. Type of Report: FINAL	**11. Date of Report:** 11 May 2004
12. Page Count: 28 (Includes Abstract, Table of Contents, Appendices and Bibliography)	
13. Supplementary Notation: A paper submitted to the Provost, Naval War College, for the AFCEA Award essay competition. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: **Information Technology; Information Technology Systems; Information Assurance and Vulnerability Assessment (IAVA); Computer Network Defense; Computer Vulnerabilities; Information System Security; Computer Security Incident; Computer Emergency Response Team (DoD-CERT); Cyberspace; Joint Task Force Computer Network Defense**	

15. Abstract:

The United States' open society, coupled with its reliance on technology and information systems, represents a vulnerability which must be protected. Both the Federal Government and the Department of Defense have focused on the problem and have made strides in improving their information assurance and vulnerability assessment processes to better protect our nation's critical information technology systems. One of the main challenges of securing our information technology systems arises from the natural characteristic of vulnerabilities; they can only be fixed once identified. The growth of the internet, as well as our nation's reliance on information technology, however, makes the task even more daunting. Computers and the internet touch almost all aspects of our lives in the United States, from banking/finance to retail to education. The time sensitivity of getting the fixes applied requires seamless coordination among the key players in the Federal Government, military, and civilian sectors. Although efforts are underway to improve the processes and coordination, there is still considerable work to be done. The current processes often leave the combatant commander out of the information loop and blind to potential problems in his theater. This paper evaluates the current Department of Defense processes and structure and offers recommendations to improve the efficiency and effectiveness of our information assurance and vulnerability assessment process.

16. Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
17. Abstract Security Classification: UNCLASSIFIED			
18. Name of Responsible Individual: Office of the Provost, Naval War College			
19. Telephone: 841-3589		**20. Office Symbol:** 01A	

NAVAL WAR COLLEGE
Newport, RI

PROTECTING OUR CRITICAL INFORMATION TECHNOLOGY SYSTEMS

By

BABETTE M. LENFANT
Lt Col, USAF

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

Advisor: _____

11 May 2004

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
14-05-2004	FINAL	

4. TITLE AND SUBTITLE

Protecting Our Critical Information Technology Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

BABETTE M. LENFANT, Lt Col, USAF

Paper Advisor: Professor Douglas N. Hime

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

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

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The United States' open society, coupled with its reliance on technology and information systems, represents a vulnerability which must be protected. Both the Federal Government and the Department of Defense have focused on the problem and have made strides in improving their information assurance and vulnerability assessment processes to better protect our nation's critical information technology systems. One of the main challenges of securing our information technology systems arises from the natural characteristic of vulnerabilities; they can only be fixed once identified. The growth of the internet, as well as our nation's reliance on information technology, however, makes the task even more daunting. Computers and the internet touch almost all aspects of our lives in the United States, from banking/finance to retail to education. The time sensitivity of getting the fixes applied requires seamless coordination among the key players in the Federal Government, military, and civilian sectors. Although efforts are underway to improve the processes and coordination, there is still considerable work to be done. The current processes often leave the combatant commander out of the information loop and blind to potential problems in his theater. This paper evaluates the current Department of Defense processes and structure and offers recommendations to improve the efficiency and effectiveness of our information assurance and vulnerability assessment process.

15. SUBJECT TERMS

Information Technology; Information Assurance and Vulnerability Assessment (IAVA); Vulnerability; Information System Security; Computer Network Defense; Computer Security Incident

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		18	19b. TELEPHONE NUMBER (include area code) 401-841-3556

Abstract

The United States' open society, coupled with its reliance on technology and information systems, represents a vulnerability which must be protected. Both the Federal Government and the Department of Defense have focused on the problem and have made strides in improving their information assurance and vulnerability assessment processes to better protect our nation's critical information technology systems. One of the main challenges of securing our information technology systems arises from the natural characteristic of vulnerabilities; they can only be fixed once identified. The growth of the internet, as well as our nation's reliance on information technology, however, makes the task even more daunting. Computers and the internet touch almost all aspects of our lives in the United States, from banking/finance to retail to education. The time sensitivity of getting the fixes applied requires seamless coordination among the key players in the Federal Government, military, and civilian sectors. Although efforts are underway to improve the processes and coordination, there is still considerable work to be done. The current processes often leave the combatant commander out of the information loop and blind to potential problems in his theater. This paper evaluates the current Department of Defense processes and structure and offers recommendations to improve the efficiency and effectiveness of our information assurance and vulnerability assessment process.

Table of Contents

List of Illustrations

Introduction

> The United States is vulnerable to sneak attacks in cyberspace that could amount to a "digital Pearl Harbor," a top government official warned on Friday. Richard Clarke, who coordinates security and infrastructure protection at the White House National Security Council, said the next U.S. president must shield the economy from foreign cyber warriors.
>
> Scott Hillis, "U.S. Could Face 'Pearl Harbor' in Cyberspace"

It's early Monday morning and everyone arrives at work on base to find the network not functioning. The network personnel are scrambling to find the problem and are soon notified by their Service's emergency response team that there has been a denial of service attack initiated from an unknown location affecting the entire Department of Defense (DoD) network. The perpetrators were supposedly able to gain access to DoD personal computers using standard password cracking software and then exploited known software vulnerabilities in Microsoft Windows to gain root access and launch a destructive virus. The DoD Computer Emergency Response Team (DoD-CERT) is working with all of the Service response teams to identify the scope of the problem and direct the recovery actions, but resolution is hours away. If the system administrator had just applied the software patches directed last month by the DoD-CERT through the Information Assurance Vulnerability Assessment (IAVA) process, the organization could have avoided this entire outage.

Although a fictitious scenario, similar events have occurred in the past and have had significant impacts. Ten years ago, people would have still been able to accomplish a lot of their work without access to E-mail or the network resources. Today, however, productivity is greatly affected. This type of network outage in a standard office environment may not be significant, but a single network outage can prove devastating to a finance company or deployed joint task force commander. Finance companies can lose millions of dollars when their systems are down. For the Joint Task Force commander, the cost could be even higher. Without the ability to access to key intelligence resources, view the common operational picture of the battlespace, or

disseminate the latest changes to the Air Tasking Order, lives could be at stake. Such incidents, as well as the asymmetric attacks on the United States on 11 September 2001, raised our awareness of the criticality and resulting vulnerability of our nation's information systems.

In the September 2002 *National Security Strategy*, President Bush outlined the United States' leadership and focus to achieve a safer and better world. He acknowledged that enemies of today no longer need great military or industrial capability. Today, terrorists and others intending harm to the United States can inflict significant damage with minimal costs by taking advantage of the openness of our society and "turn[ing] the power of modern technologies against us."[1]

The United States' open society, coupled with its reliance on technology and information systems, represents a vulnerability which must be protected. *Joint Vision 2020* acknowledges that "Information, information processing, and communications networks are at the core of every military activity."[2] This dependence is also evident in most of our civilian activities and increases as internet availability and use rises. Current statistics from 6 April 2004 showed over 350 million people in the world use the internet. The internet has penetrated over 11 percent of the world's population, with a user growth of 106.3 percent from 2000 to 2004.[3] Computers and the internet touch almost all aspects of our lives in the United States, from banking/finance to retail to education.

Inline with the growth of the general public's use of the internet, the United States Federal Government has become increasingly reliant on the internet and computer networks. It has automated many services in an effort to save precious resources, as well as improve

---

[1] White House, *National Security Strategy of the United States of America*, September 2002, Washington, D.C.: GPO, 2002, Preface note from George Bush.

[2] Department of Defense, *Joint Vision 2020*, Washington, D.C.: GPO, 2000, 8. Internet, online available at http://www.dtic.mil/jointvision/jv2020.doc. Accessed 30 March 2004.

[3] "Internet Usage Statistics The Big Picture," Internet World Stats Usage and Population Statistics, Internet, online, available at http://www.internetworldstats.com/stats.htm. Accessed 25 April 2004.

efficiency. People can file their income tax returns electronically, purchase government bonds on-line and access their federal pay information. The United States military has also capitalized on the power of computer networks to improve its access to intelligence resources, information dissemination, and battlefield awareness. With this increased reliance on the computer networks and the openness of our society, however, comes an increased vulnerability.

The United States' political and military leadership understand that continued access to critical computer network resources must be a priority and have established several organizations to spearhead the efforts to protect our systems. One of the main problems, however, arises from the natural characteristic of vulnerabilities; they can only be fixed once identified. Another problem is that vulnerabilities are often first identified by those trying to exploit systems. Today, these vulnerabilities are often published with tools to exploit them, reducing the time system administrators have to react to apply the necessary fix actions.[4] The time sensitivity of getting the fixes applied requires seamless coordination among the key players in the Federal Government, military, and civilian sectors. Although efforts are underway to improve this coordination, there is still considerable work to be done.

This paper will discuss the reasons why the United States should be concerned about this problem and will highlight the Federal Government and military organizations and processes currently in place to address these problems. It will then delve into a more detailed analysis of the current military organizations, highlighting the impact of the current structure on the combatant commander. Finally, the paper will offer recommendations and highlight the need for more standardized systems and processes, as well as better coordination within the Department of Defense and among federal organizations.

---

[4] "Symantec Internet Security Threat Report", Volume V, Published March 2004, 1, Internet, online, available at http://wwwsoftmart.com/symantec/documents/Internet_Threat_Report_Exec_Summ_3-22-04.pdf. Accessed 25 April 2004.

This paper focuses on the information assurance and vulnerability assessment aspects of defensive information operations and does not address the equally important topic of the United States' ability to deny our adversaries access to their systems through offensive information operations. Superior information assurance and vulnerability assessment processes are necessary to ensure continued access to critical computer systems. Our computer networks remain only as strong as the weakest link. All it takes is one system administrator to fail to apply the required fix in a timely manner. To use the analogy of a house, locking all of the doors and the garage, but forgetting to secure just one window leaves the house vulnerable to an attack.

Reason for Concern

According to the Computer Emergency Response Team, Coordination Center (CERT/CC) the number of reported computer incidents and vulnerabilities, as well as the economic impact, has grown significantly over the years (Figures 1 and 2). What raises our concern even more is that several industry surveys suggest that 50-80 percent of incidents go unreported.[5]

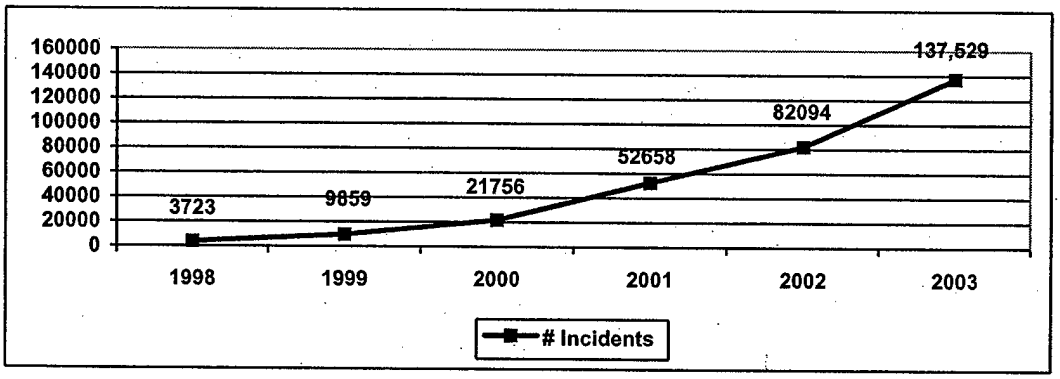

Figure 1: Reported Computer Security Incidents, 1998-2003[6]

[5] Computer Emergency Response Team (CERT) Coordination Center, CERT/CC Statistics, 1988-2003, 1, Carnegie-Mellon University, Internet, online, available at http://www.cert.org/stats/cert_stats.html. Accessed on 30 March 2004

[6] Ibid, 1.

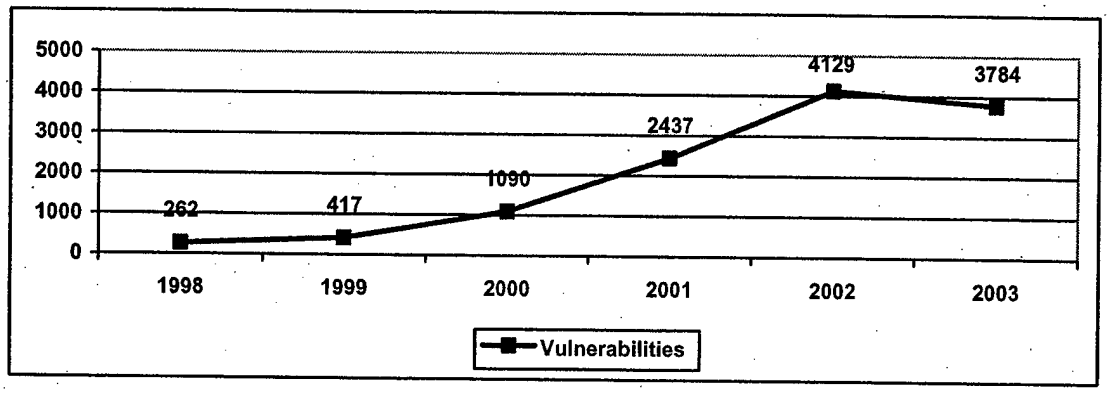

Figure 2: Vulnerabilities Reported 1998-2003[7]

The Symantec Internet Security Threat Report highlighted that the most significant events occurred in August 2003, when the Internet experienced three new high-threat worms in only twelve days. Blaster, Welchia, and Sobig.F infected millions of computers throughout the world and may have caused over $2 billion in damage.[8] "Trend Micro, the world's third-largest anti-virus software maker," estimated the economic impact of virus attacks on global businesses for 2003 to be $55 billion in U.S. dollars. This is a 175 percent increase from the estimated $20 billion impact in 2002, and the impact is expected to rise in 2004.[9]

Every vulnerability represents a potential access point into our critical computer systems. With more than ten new vulnerabilities identified each day in 2003,[10] trying to keep all of the systems updated with the latest patches is a monumental task for system administrators, and this is only one of their responsibilities. The importance of United States computer systems, as well as the scope and potential impact of incidents highlights why the United States needs to be concerned. The Federal Government and the Department of Defense have both taken steps to better address these threats. First we will look at the Federal Government's efforts.

---

[7] Ibid, 1.

[8] "Symantec Internet Security Threat Report," 1.

[9] "2003 Computer Viruses Damage Put at US55b." *China Daily Online.* January 17, 2004. http://www.chinadaily.com.cn/en/doc/2004-01/17/content_299897.htm. Accessed on 25 April 2004.

[10] Extrapolated by author from CERT/CC Statistics, 1988-2003. With 3784 new vulnerabilities per year, this averaged out to be over 10 a day for 365 days.

Federal Government Efforts and Current Structure

The national policy on computer network defense has been evolving since the mid-1990s. The key legislation and initiatives are outlined in Figure 3.

Directives/Policies	Year	Summary
Executive Order 13010	1997	Defined critical infrastructures; Established Critical Infrastructure Protection Commission
Presidential Decision Directive 63	1998	Established infrastructure protection as national goal; created Critical Infrastructure Protection Office (CIPO) under Dept of Commerce and National Infrastructure Protection Center (NIPC) under FBI; Created National Infrastructure Assurance Council to facilitate private/public sector cooperation; established lead agencies for specific segments
National Plan for Infrastructure Protection	2001	Focused Federal efforts, required vulnerability assessments for each segment; linked funding approvals to information security plans; directed establishment of a national warning center for infrastructure attacks (filled by NIPC)
Executive Order 13231	2001	Established President's Critical Infrastructure Protection Board (PCIB) chaired by Special Advisor to the President on Cyberspace Security to coordinate Federal efforts to protect national infrastructures; 10 standing committees – Coordinates with Office of Homeland Security on attacks against U.S. information infrastructure
Executive Order 13238	2001	Establishes Office of Homeland Security to develop comprehensive strategy to secure U.S. from attacks
Creation of Department of Homeland Security	2002	Created Department of Homeland Security and assigned the Secretary of DHS the responsibilities for cyberspace security
National Strategy to Secure Cyberspace	2003	Establishes collaborative effort between Federal and private sector lead agencies, and provides specific recommendations for each major infrastructure segment to secure U.S information systems against attack
National Cyber Alert System	2004	Jan 2004, The National Cyber Security Division of the Department of Homeland security unveiled the National Cyber Alert System to provide Americans timely and actionable information to better secure their computer systems. To identify, analyze and prioritize emerging vulnerabilities and threats

Figure 3: Key Government Legislation and Policies[11]

The 11 September 2001 attacks made the United States more aware of its vulnerabilities and led to the most significant policy changes. Understanding the United States' reliance on information infrastructure, the President identified the need for an agency to coordinate and monitor the federal efforts and programs to ensure protection of the country's information infrastructure. With Executive Order 13231, the President created the Critical Infrastructure Protection Board to promote information sharing and coordination with the private sector, state

[11] Compiled by author summarizing key aspects of the federal government publications. The individual documents are accessible from http://iase.disa.mil/policy.html. Accessed on 25 April 2004.

and local governments, and corporate and academic organizations in order to improve the security of the information infrastructure, as well as incident response.[12] In December 2002, the Department of Homeland Security was created to focus specifically on reducing the vulnerabilities of the United States. As part of its mission, the Department of Homeland Security was assigned the responsibilities for cyberspace security. The United States Computer Emergency Readiness Team (U.S. CERT) was established under the Department of Homeland Security and was charged with protecting our nation's Internet infrastructure by coordinating defense against and response to cyber attacks.[13]

In February 2003, the President released the *National Strategy to Secure Cyberspace.* The purpose of the document was to "engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact."[14] Securing cyberspace, however, requires a coordinated effort across all areas of society. Although the document offered suggestions to business, academic institutions and individual users, it contained no mandates. This was an important step, but there is still an enormous amount of work to be done in developing a coherent process to identify and track vulnerabilities.

In January 2004, the Department of Homeland Security unveiled the National Cyber Alert System, which categorizes computer security alerts and provides warning and update information to allow all citizens to better protect their vulnerability to attacks from cyberspace.[15] These efforts have improved the availability and access to information about potential problems, as well as the communication flow. However, there are still no teeth behind the Federal

---

[12] White House, "Executive Order 13231-Critical Infrastructure Protection in the Information Age," *Federal Register*, October 18, 2001, Vol. 68, No 18, Washington, D.C.: GPO, 2001, 53063, Internet, online, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname2001_register&docid=fr18oc01-139.pdf. Accessed 30 March 2004.

[13] U.S. CERT homepage, Internet, online, available at http://www.us-cert.gov/. Accessed on 25 April 2004.

[14] White House, *The National Strategy to Secure Cyberspace*, February 2003, Washington, D.C.: GPO, 2003, Executive Summary, Internet, online, available at http://www.whitehouse.gov/pcipb/. Accessed on 30 March 2004.

[15] U.S. Department of Homeland Security, *U.S. Department of Homeland Security Improves America's Cyber Security Preparedness – Unveils National Cyber Alert System*, by Donald Tighe, U.S. Department of Homeland Security Announcement, Internet, online, available at http://www.us-cert.gov/press_room/cas-announced.html. Accessed 25 April 2004.

Government's "suggestions," nor any mandates or timelines. Unfortunately, the security of our national systems continues to rely on the willingness and competence of computer network employees and is only as secure as the weakest link. In conjunction with the Federal Government's programs, the DoD has continued to focus on improving its information assurance processes.

DOD Efforts and Current Structure

Secretary Rumsfeld in the *Quadrennial Defense Review Report*, September 30, 2001, highlighted as one of the six critical operational goals, "assuring information systems in the face of attack."[16] The importance of defending our critical information systems was not a new concept to the DoD. In fact, *Joint Vision 2010*, stated that the United States' ability to achieve its goal of full spectrum dominance, rests on the foundations of information superiority.[17] Each of the Services had already established its own network operation and security centers, and the Defense Information Systems Agency (DISA) had established an overarching Global Network Operations and Security Center (GNOSC) to provide guidance and limited oversight. Defense exercises and real world events in 1997 and 1998, however, highlighted the need for a single organization within the DoD to coordinate defensive actions and direct recovery efforts in the event of an attack.

In December 1998, the Department of Defense established the Joint Task Force Computer Network Defense (JTF-CND) to serve as the DoD focal point.[18] The Unified Command Plan 1999 assigned both the computer network attack (CNA) and CND missions to

---

[16] U.S. Department of Defense, *Quadrennial Defense Review Report*, September 30, 2001, Washington, D.C.: GPO, 2001, 30.

[17] U.S. Department of Defense, *Joint Vision 2010*, Washington, D.C.: GPO, 2001, 17, Internet, online, available at http://www.dtic.mil/jv2010/jv2010.pdf. Accessed 30 April 2004.

[18] U.S. Department of Defense, DoD News Release, Number 658-98, *Joint Task Force on Computer Network Defense Now Operational*, 30 December 1998, Internet, online, available from http://www.defenselink.mil/news/Dec1998/b230198_bt658-98.html, accessed 30 March 2004.

United States Space Command (USSPACECOM). USSPACECOM commissioned a study to determine the feasibility of integrating these missions under one task force. Determined feasible, JTF-CND was re-designated Joint Task Force-Computer Network Operations (JTF-CNO) on 2 April 2001. With the merger of USSPACECOM and United States Strategic Command (USSTRATCOM) on 1 October 2002, JTF-CNO was reassigned to USSTRATCOM. JTF-CNO is responsible for coordinating and directing the defense of DoD computer systems and networks, and directing appropriate actions through its four military Service components and the DoD Computer Emergency Response Team (DoD-CERT) for each Service's computer emergency response team.[19]

JTF-CNO is co-located and supported by the Defense Information Systems Agency (DISA) Global Network Operations and Security Center (GNOSC). This collocation allows JTF-CNO visibility into the status of the Defense Information Infrastructure (DII), 24-hours a day 7-days a week.[20] JTF-CNO also takes advantage of existing intrusion detection capabilities at the unified commands, components and DoD agencies to identify any potential problems, correlate the information to determine the impact on operations, develop courses of action to address the threat, and direct necessary recovery actions. Although JTF-CNO was designated as the single DoD agency to coordinate and direct actions, each combatant commander, Service, and agency was tasked to develop its own processes to ensure the security of its systems. The disparate efforts of these organizations have led to some of the coordination problems and issues that exist today.

---

[19] U.S. Strategic Command Fact Sheet, *Joint Task Force –Computer Network Operations*, Internet, online, available from http://www.stratcom.mil/factsheetshtml/jtf-cno.htm, accessed 30 March 2004.

[20] DoD News Release, Number 658-98.

Evaluation of Current DoD Processes/Structure[21]

Figure 4 summarizes some of the current key policy documents on information operations and the information assurance and vulnerability assessment aspects of computer network defense. Overall, the policies across DoD are not consistent. The Services, as directed, developed their own processes and procedures for ensuring the security of their systems, and this led to conflict between the Services and combatant commands on how the reporting and monitoring process should be done.

Documents	Year	Summary
JP 3-13; Joint Doctrine for IO	Oct 1998	Defies the objectives of information operations, including offensive and defensive (IO); gives guidance concerning IO planning, org and training issues
DoD Information Assurance Vulnerability Alert (IAVA) Process	1998	Instituted in 1998 to provide DoD positive control of vulnerability notification and corresponding corrective action. DISA assigned to manage the IAVA process, distribute alerts to all Combatant commands, Services, agencies
DoD Directive O-8530.1; Computer Network Defense (CND)	Jan 2001	Established the CND policy, definitions and outlined responsibilities. Assigned overall responsibility to SPACECOM (at the time) for CND within DoD information systems and computer networks
CJCSM 3150.07A IAVA Process	April 2001	Established process to provides the Joint Staff, combatant commands, Services, and defense agencies pertinent information concerning conditions that impose serious degradation of communications operations in DoD network.
CJCSI 6510.01C IA and CND	May 2001	Focused on the policy and responsibilities for implementing IA defense-in-depth strategy and CND for SPACECOM (at the time). Directed establishment of DoD CERT to centrally coordinate actions involving incidents and vulnerabilities (First tier support). Tasked Services to develop second tier capability and processes. Tasked DISA to lead development/implementation of single IA concept for layered protection
DoD Directive Number 8500.1 IA	Oct 2002	Established policy and assigns responsibilities under the Defense Information Assurance Program to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology. DISA tasked to develop, implement and oversea a single IA approach
DoD Instruction Number 8500.2; IA Implementation	Feb 2003	Implemented policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.1.
Joint Concept of Operations for Global Information Grid NetOps	Draft Feb 2004	Establishes the Joint Mission Essential Tasks and Command and Control structure that will be used to conduct STRATCOM's Global NetOps mission as assigned in Change 2 to the Unified Command Plan 2002

Figure 4: DoD Doctrine and Instructions on IAVA[22]

[21] This evaluation represents a summary of issues compiled through interviews identified in the bibliography (Brown, Burgess, Hunninghake, Oliver and Valdez), as well as the author's personal experience as a communications squadron commander.

[22] Compiled by author as summary of the key Department of Defense publications available on the information assurance and vulnerability assessment process. All of the documents are accessible from http://iase.disa.mil/policy.html. Accessed 5 April 2004.

IAVA distribution and tracking process

Currently, IAVAs are forwarded from the DoD-CERT through JTF-CNO by message, email and secure internet to the combatant commands and the Services' emergency response teams, with an established date for compliance. The Services then reissue the IAVA (sometimes with their own unique number) and establish their own deadline to organizations for which they are responsible. Service components, which are part of a combatant command, or bases that are part of a subunified command, are left trying to determine which IAVAs are related and to which they must respond, causing frustration. An example of the convoluted reporting requirements for PACOM/PACAF units is identified in Figure 5.

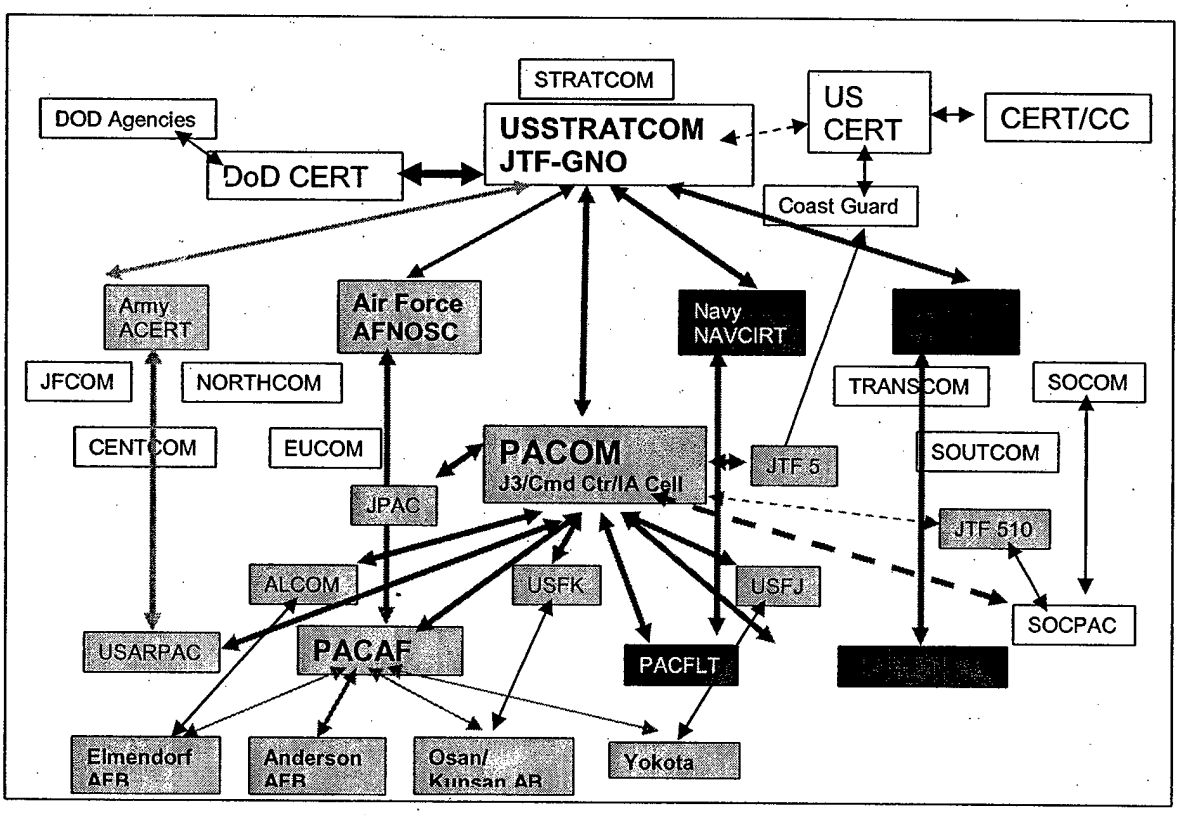

Figure 5: Example IAVA Reporting Requirements for PACOM/PACAF Units[23]

[23] Diagram created by author from personal knowledge and information gained from interviews. Diagram's accuracy verified by Brown, Jeffrey, JTF-CNO on 26 April 2004.

Resource Impact of Fixing Vulnerabilities

These processes are compounded by the number of IAVAs received. As stated previously, CERT/CC identifies or is informed of at least ten new vulnerabilities daily. Although some may not impact any DoD systems, others may affect every computer. The process for resolving the IAVAs and updating the appropriate IAVA monitoring systems can be time consuming. For example, each time there is a software patch for Internet Explorer or one of the other standard software packages used across DoD, the patch must be applied to every system running the software. New patches can be released on the same software packages each month, requiring the similar actions to be taken again. Although some of the Services/bases have automated a portion of the software update process, this is not true across the Services. Even for those bases with the automated system, most develop similar software scripts to execute the update process instead of the generic scripts being created at the highest level, requiring only minor modifications. Government Off-the-Shelf (GOTS) software causes additional concerns.

Patches to standard commercial software can affect the functioning of key GOTS; therefore, updates to systems running the GOTS cannot be completed until the software package is modified. Since program managers are currently judged on cost and schedules rather than IAVA compliance, the vulnerabilities are often left open for often months. Without standardized reporting and tracking systems, statistics on compliance could be suspect.

Defining Compliance

What should be the true measure of compliance? Trying to maintain 100 percent compliance all of the time is not feasible, so what is the acceptable level of risk? With over ten new vulnerabilities identified each day, there will always be some vulnerabilities not yet patched. U.S. CERT's development and release of the new Cyber Alert System, in January 2004, may

help better define acceptable levels of compliance and help prioritize the efforts of information technology (IT) personnel. The most critical vulnerabilities must be addressed quickly.

CND Incident Reporting Process

Beyond the IAVA process, the combatant commands are also frustrated with the current CND incident reporting process. Defining what constitutes an incident has problematic in and of it self. Although there are DoD instructions outlining what should be reported, and JTF-CNO has provided additional guidance, the Services often interpret the guidance differently. Any virus incident on a DoD computer is required to be reported to the JTF-CNO, but, in practice, some of the Services have established different thresholds. For example, a Service may not report a virus unless it affects more than X computers on one base or affects more than X bases.

Once an incident has occurred, the current process calls for the affected Service(s) to report the incident through its/their Service channel(s), through DoD-CERT to JTF-CNO. Although the flow makes sense considering the Services own the preponderance of assets, have global views of their systems, and are therefore better able to filter erroneous indications, Service reporting often leaves the combatant command out of the information loop. The Service components are supposed to report incidents to their regional combatant commanders in parallel, but this does not always happen. This reporting structure leaves the regional commanders potentially blind to what is occurring in their theaters. The combatant commands are now trying to change the process and force JTF-CNO to issue direction through them to the Service components. Although this would improve a combatant commander's visibility, it creates other issues about how to handle areas and bases not aligned with a specific combatant command. Moreover, many of the combatant commands lack a robust structure within their staffs to handle this process.

Interagency Incident Coordination and Resolution Process

Often incidents are not limited to DoD systems only. The U.S. CERT was established to monitor incidents and direct the resolution affecting the federal government, as well as interface with non-government organizations. The interfaces between U.S. CERT and the federal organizations, DoD and the civilian sector have not been formalized. Phone communication remains the key ingredient between the JTF-CNO and U.S. CERT organizations. A true test of how well the organizations function together will only occur with exercises or a real world event.

Personnel Concerns

Related to the lack of resources on the combatant commander's staffs is the disparity in IT experience and expertise within and among the Services. The system administrators are one of the most important keys to maintaining the security of the DoD information systems, however, there is no standardized training across the Services. The Services are also finding it difficult to keep trained personnel with the availability of high paying jobs in the civilian sector. As a result of personnel shortages, updating information systems to remedy vulnerabilities is sometimes tasked to administrative personnel as an additional duty. Since the overall security of a system remains only as strong as the most vulnerable point, it seems questionable that we would want this responsibility to be an additional duty. The current push to outsource or consolidate many of the IT functions as a result of personnel concerns, also raises other issues.

Sources of attacks on IT systems can originate from inside or outside. Although military personnel or government civilians cannot be discounted as potential saboteurs, contracting out IT functions adds a new dimension and requirements for adequate screening. Outsourcing these responsibilities also limits the number of trained personnel available to handle similar tasks in a deployed environment. The same is true for consolidating many of the higher level system

administration functions. The IT personnel on a base who do not perform the IT functions on a daily basis, find it difficult to remain proficient in these tasks and require additional training prior to deployment.

Recommendations

In December 2003, the DoD announced the planned merger of the Defense Information Systems Agency's (DISA) directorate of operations and JTF-CNO to form Joint Task Force Global Network Operations (JTF-GNO), which will handle both network defense and network management. DISA' GNOSC will become the Global Network Center (GNC) and be subordinate to JTF-GNO. JTF-GNO is tasked with the global management and defense of the DoD's information infrastructure.[24] Given these responsibilities, and the fact that vulnerabilities and incidents can affect many different government and civilian systems, JTF-GNO will have to develop a more formal relationship with U.S. CERT. A smooth interface and flow of information between the organizations will allow a better understanding of the potential impacts and status of resolution efforts. I recommend each organization establish a formal liaison officer position within its organization.

Internal to the DoD, JTF-GNO will have to determine who should ultimately be responsible for the subordinate IAVA process, the Services or the combatant commands. Although the combatant commands are pushing to be the focal points, I believe the Services, with some modifications in processes, are better equipped to continue handle the responsibility. The Services are responsible for organizing, training, and equipping their forces in support of the combatant commands. It seems logical that the IAVA process fall under this purview, especially since all of the Services already have organizations in place to handle the IAVA process.

---

[24] Donald Tighe, U.S. Department of Homeland Security Announcement; Col Jeffrey Brown interview.

Conversely, most of the combatant commands would have to pull resources from their staffs or from the Services to handle the responsibility, creating duplication of effort and inefficient use of resources. If JTF-GNO and the Services were able to provide a theater view of the IAVA status for the combatant commander as part of his common operational picture, then does the combatant command actually need to control the process? Providing visibility into the status of IAVAs and vulnerabilities, as well as a reachback capability for deployed commanders should meet the requirements.

JTF-GNO currently has a liaison officer at each of the combatant commands. It is obvious from the frustration level of the combatant commands, however, that the current structure is not meeting their needs. If the decision is made to let the combatant commands serve as the focal point, JTF-GNO must assist with establishing standard organizations across the combatant commands. A couple of the combatant commands have already created regional communications coordination centers to monitor the status of their critical IT systems. DISA also has regional coordination centers as well. It is important that JTF-GNO look at existing capabilities and challenges to determine the best structure and processes. Regardless of whom the DoD decides should own the subordinate process, the current systems are inadequate and inefficient to provide the capabilities required and must modified.

A single consolidated tracking system must be developed to track IAVA distribution and resolution. Even if the U.S. CERT system which lists the current vulnerabilities and criticality cannot be expanded, a consolidated DoD system should be developed. Since some bases and Services are doing better than others at tracking and reducing vulnerabilities, the DoD should evaluate all of the existing Service systems/processes to identify the best practices. Once identified, the systems/processes could be updated/modified to provide new capabilities. One of

the new capabilities required would be the ability to allow different views, depending on which organization is viewing the information. For example, a base commander should be able to view the status of compliance for his/her base, the Air Force the status of any Air Force base or its entire Service (broken out by major command or base as requested), and the combatant command the status of its entire command or any organization falling under its responsibility. The system should send automatic notifications of new incidents or status updates to any organization that needs to be notified. If constructed correctly, the information would only have to be entered once at the source and not multiple times into separate systems. One DoD system with flexible views would significantly reduce the duplication of effort across the Services. The long-term goal, however, should remain the development of one consolidated system for the entire federal government.

Another important requirement of the consolidated system would be the ability to differentiate between the criticality of the IAVAs, similar to the U.S. CERT's National Cyber Alert System. When determining the criticality of an IAVA or incident, the system needs to take into account two parameters, the criticality of the system affected and the potential destructiveness if the vulnerability was exploited. Knowing the criticality, the IT personnel could better prioritize their resolution efforts. Mandates on how long an organization has to correct the vulnerabilities would be established for each level of criticality.

Another way to improve the efficiency of the IT personnel is greatly reduce the time required to correct vulnerabilities. Implementing standard software update capabilities and providing training to the IT personnel on the system would significantly reduce the time required. Automatic software distribution and update packages exist today and have been implemented at some DoD locations. These tools can automatically correct software

vulnerabilities as soon as a person logs on in the morning. The problem remains that today, the tools are not standardized and the implementation is not widespread. A standard software tool must be selected and implemented at each location. Centralizing the creation of update scripts at DoD-CERT would also facilitate the vulnerability correction process. DoD-CERT would be responsible for developing the standard scripts and organization could make any minor modifications to account for the uniqueness of its location. The scripts would be available right next to the vulnerability description and update status on the identification and tracking web site. Standardized systems and procedures across the Services would streamline training, and provide the joint task force commanders more flexibility on the use of their critical IT personnel.

Overall, the Federal Government and DoD have made strides in improving the security of our nation's critical IT systems. Implementation of the actions discussed above would improve the IAVA process even more and help reduce the existing vulnerabilities in federal IT systems. Implementation of standardized systems for tracking and updating vulnerabilities and incidents, which allow commanders at every level the required visibility, would reduce the combatant commanders' frustration. In addition, liaisons at both U.S. CERT and JTF-GNO would facilitate the coordination and resolution processes for critical widespread incidents. Implementation of standardized IAVA procedures and standardized automated software update tools would also reduce the dissatisfaction of the IT personnel and allow them time to focus on their other responsibilities. Further research is required into the appropriate systems and tools and the best processes, but I believe implementing these recommendations would go a long way toward mitigating or preventing the scenario depicted in the introduction.

Appendix A: Acronyms

CERT/CC – Computer Emergency Response Team Coordination Center
CNA – Computer Network Attack
CND – Computer Network Defense
DII – Defense Information Infrastructure
DISA – Defense Information Systems Agency
DoD – Department of Defense
DoD CERT – Department of Defense Computer Emergency Response Team
GIG – Global Information Grid
GNC – Global Network Center
GNOSC – Global Network Operations and Security Center
IAVA – Information Assurance Vulnerability Assessment
IO – Information Operations
JTF-CND – Joint Task Force – Computer Network Defense
JTF-CNO – Joint Task Force – Computer Network Operations
JTF-GNO – Joint Task Force – Global Network Operations
NCSD – National Cyber Security Division; charged with coordinating the implementation of the national Strategy to Secure Cyberspace and serves as the single National point of contact for the public and private sector regarding cyber security issues. Also charged with identifying, analyzing and reducing cyber threats and vulnerabilities; disseminating threat warning information; coordinating incident response; and providing technical assistance in continuity of operations and recovery planning
U.S. CERT – United States Computer Emergency Readiness Team; part of NCSD; serves as a focal point – bridging public and private sector institutions to advance computer security preparedness and response
UCP – Unified Command Plan
USSPACECOM – United States Space Command
USSTRATCOM – United States Strategic Command

Appendix B: Glossary

Computer Network Defense – includes measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

Computer Emergency Response Team, Coordination Center (CERT/CC) - established in 1988 by the Defense Advanced Research Projects Agency (DARPA) in 1988 after a computer worm disabled about 10% of all computers connected to the internet. CERT/CC is located at the Software Engineering Institute, a federally funded research center operated by Carnegie Mellon University. CERT/CC studies internet security vulnerabilities.

Incident – act of violating an explicit or implied security policy. Include but are not limited to: attempts to gain unauthorized access to a system or its data; unwanted disruption or denial of service; the unauthorized use of a system for the processing or storage of data; changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Information Assurance (IA) – I[nformation] O[perations] that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [JP 3-13] In other words, information assurance is everything done to ensure our information systems are available for use by authorized users, that they work the way they are suppose to and that only authorized users are available to use and get information from them.

Information Superiority – the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting, or denying an adversary's ability to do the same. (JP1-02)

Vulnerability - any weakness in a system that allows unauthorized intruders to gain unauthorized access to a system and/or process.

Selected Bibliography

"2003 Computer Viruses Damage Put at US$55b." *China Daily On-Line*, January 17, 2004. http://www.chinadaily.com.cn/en/doc/2004-01/17/content_299897.htm. Accessed on 25 April 2004.

Briefing to the JCS by RADM Richard W. Hunt, Deputy Directory for Strategy and Policy, *2004 National Military Strategy*, 13 February 2004.

Brown, Jeffrey C., of JTF-CNO. Interviewed by author via email several times between 29 March and 28 April 2004.

Burgess, Keith, Deputy Commander, NAVCIRT. Interviewed by author via email several times between 15 April and 28 April 2004.

Computer Emergency Response Team (CERT) Coordination Center, *CERT/CC Statistics, 1988-2003*, Carnegie-Mellon University, Internet, on-line, available at http://www.cert.org/stats/cert_stats.html. Accessed on 30 March 2004.

Foote, Darlene M. "SSG Division Keeps Air Force Bases Connected," United States Air Force News Release, Release No. 03-12-38, 1 December 2003, Internet, on-line, available at https://web1.ssg.gunter.af.mil/home/documents/03-10-38AFNOCKeepsBases Connected.pdf. Accessed 30 March 2004.

Hillis, Scott. "U.S. Could Face 'Pearl Harbor' in Cyberspace." *Daily News*, 8 December 2000. http://www.merit.edu/mail.archives/netsec/2000-12/msg00024.html. Accessed on 30 March 2004.

Holdaway, Eric J. "Active Computer Network Defense, An Assessment", April 2001, Internet, on-line, available at http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students /2001/01-055.pdf. Accessed on 30 March 2004.

Hunninghake, David of Air Staff, Pentagon, Washington D.C. Interviewed by author via email several times between 15 and 28 April 2004.

"Internet Usage Statistics The Big Picture." Internet World Stats Usage and Population Statistics, Internet, on-line, available at http://www.internetworldstats.com/stats.htm. Accessed 25 April 2004.

Jenkins, James A. "Computer Network Defense, DOD and the National Response", 2 December 2002, Internet, on-line, available at http://www.au.af.mil/au/awc/awcgate /awc/jenkins.pdf. Accessed 30 March 2004.

Oliver, Eric P. Operations Officer at the Air Force Network Operations and Security Center, Barksdale AFB, LA. Interviewed by author via email several times between 15 and 28 April 2004.

Richardson, Robert. "2003 CSI/FBI Computer Crime and Security Survey", Published by Computer Security Institute, Internet, on-line, available at http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf. Accessed 30 March 2004.

"Symantec Internet Security Threat Report", Volume V, Published March 2004, Internet, on-line, available at http://wwwsoftmart.com/symantec/documents/Internet_Threat_Report_Exec_Summ_3-22-04.pdf. Accessed 25 April 2004.

Tuttle, Rich. "DISA Director's Impending STRATCM Job Seen Helping Network Acquisition." *Aerospace Daily*, 25 March 2004. http://ebird.afis.osd.mil/ebfiles/s20040425270038.html. Accessed on 25 March 2004.

U.S. Army Regulation 25-2, *Information Management, Management of Subdisciplines, Information Assurance*, 14 Nov 2003, Washington, D.C.: GPO, 2003, Internet, on-line, available at http://www.usapa.army.mil/pdffiles/r25_2.pdf. Accessed 30 March 2004.

U.S. Army Regulation 380-53, *Security, Information Systems Security Monitoring*, Washington, D.C.: GPO, 1998, Internet, on-line, available at http://www.usapa.army.mil/pdffiles/r380_53.pdf. Accessed 30 March 2004.

"U.S. Business Cyber Security study", conducted by the Business Software Alliance, 24 July 2002, Internet, on-line, available at http://global.bsa.org/security/resources/2002-07-24.pdf?CFID=146648&CFTOKEN=49679927. Accessed on 30 March 2004.

U.S. Department of Defense, CJCSI 3401.03A, *Information Assurance and Computer Network Defense: Joint Quarterly Readiness Review Metrics*, 15 July 2003, Washington, D.C.: GPO, 2003, Internet, on-line, available at http://www.dtic.mil/cjcs_directives/cdata/unlimit/3401_03.pdf. Accessed 30 March 2004.

U.S. Department of Defense, CJCSI 6510.01C, *Information Assurance and Computer Network Defense*, 1 May 01, Washington, D.C.: GPO, 2001.

U.S. Department of Defense, CJCSM 3150.07A, *Joint Reporting Structure Communications Status*, 19 April 2001, Washington, D.C.: GPO, 2001, Internet, on-line, available at http://www.dtic.mil/doctrine/jel/cjcsd/cjcsm/m315007a.pdf. Accessed 30 March 2004.

U.S. Department of Defense, *The Department of Defense Information Assurance Strategic Plan*, no date, Internet, on-line, available at https://infosec.navy.mil/pub/docs/documents/dod/dodd/dod_ia_strategic_plan.pdf. Accessed 30 March 2004.

U.S. Department of Defense, *DISA IAVA Process Handbook*. Version 2.1, Dated 11 June 2002, Washington, D.C.: GPO, 2001, Internet, on-line, available at https://iase.disa.mil/IAalerts/iavahnbk.pdf. Accessed 30 March 2004.

U.S. Department of Defense, DoD Directive 8500.1, *Information Assurance (IA)*, dated October 24, 2002 (Certified current as of November 21, 2003), Internet, on-line, available at http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf. Accessed 30 March 2004.

U.S. Department of Defense, DoD Directive 8500.2, *Information Assurance (IA) Implementation*, dated February 6, 2003, Internet, on-line, available at http://www.dtic.mil/whs/directives/corres/pdf/i85002_020603/i85002p.pdf. Accessed 30 March 2004.

U.S. Department of Defense, DoD News Release, Number 658-98, "Joint Task Force on Computer Network Defense Now Operational," 30 December 1998, on-line, Internet, available from http://www.defenselink.mil/news/Dec1998/b230198_bt658-98.html. Accessed 30 March 2004.

U.S. Department of Defense, Joint Publication J1-02. *Department of Defense Dictionary of Military and Associated Terms*, 7 May 2002, Washington, D.C.: GPO, 2002.

U.S. Department of Defense, *Joint Vision 2010.* Washington, D.C.: GPO, date unknown, Internet, on-line, available at http://www.dtic.mil/jv2010/jv2010.pdf. Accessed 30 April 2004.

U.S. Department of Defense, *Joint Vision 2020.* Washington, D.C.: GPO, 2000, Internet, on-line available at http://www.dtic.mil/jointvision/jv2020.doc. Accessed 30 March 2004.

U.S. Department of Defense, "Memorandum on Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)" 30 Dec 1998, Internet, on-line, available at http://www.cert.mil/pub/bulletins /iava/iavamemo.pdf. Accessed 30 March 2004.

U.S. Department of Defense, *Quadrennial Defense Review Report*, September 30, 2001, Washington, D.C.: GPO, 2001, Internet, on-line, available at http://www.defenselink.mil/pubs/qdr2001.pdf. Accessed 30 March 2004.

U.S. Department of Homeland Security, *U.S. Department of Homeland Security Improves America's Cyber Security Preparedness – Unveils National Cyber Alert System*", by Donald Tighe, U.S. Department of Homeland Security Announcement, Internet, online, available at http://www.us-cert.gov/press_room/cas-announced.html. Accessed 25 April 2004.

U.S. Marine Corps Order, 5239.2, *Marine Corps Information Assurance Program (MCIAP)*, 18 Nov 02, Internet, on-line, available at http://www.usmc.mil/directiv.nsf/56ec379292979da685256bd0006c696e/c5fc1e22106b5b3485256cb0004b8ae8/$FILE/MCO%205239.2.pdf. Accessed 30 March 2004.

U.S. Strategic Command Fact Sheet, *Joint Task Force –Computer Network Operations*, Internet, on-line, available from http://www.stratcom.mil/factsheetshtml/jtf-cno.htm. Accessed 30 March 2004.

Valdez, Jorge R. of Marine Corps Network Operations and Security Command, Washington, D.C. Interviewed by the author via email on 29 April 2004.

White House, "Executive Order 13231-Critical Infrastructure Protection in the Information Age." *Federal Register*, October 18, 2001, Vol. 68, No 18, Washington, D.C.: GPO, 2001, Internet, on-line, available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname2001_register&docid=fr18oc01-139.pdf. Accessed 30 March 2004.

White House, "Executive Order 13284 Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security." *Federal Register*, January 23, 2003; Federal Register, Vol. 68, No. 18, Washington, D.C.: GPO, 2003, Internet, on-line, available at http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/pdf/03-2069.pdf. Accessed 30 March 2004.

White House, *National Security Strategy of the United States of America*, September 2002, Washington, D.C.: GPO, 2002.

White House, *The National Strategy to Secure Cyberspace*, February 2003, Washington, D.C.: GPO, 2003, Internet, on-line, available at http://www.whitehouse.gov/pcipb/. Accessed on 30 March 2004.

Wilson, Peter A. "Cyberwarfare and Cyberterrorism: Implications for DOD R&D", Internet, on-line, available at http://www.aaas.org/spp/yearbook/2002/ch17.pdf. Accessed on 30 March 2004.