REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this 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 this 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 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 any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2009	FINAL	

4. TITLE AND SUBTITLE
Joint Interagency Coordination Group – Cyber: Empowering the Combatant Commanders against the no-borders threat

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Osvaldo Ortiz, MAJ, USA

Paper Advisor (if Any): Stephanie Helm, CAPT, USN

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
Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations 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 worldwide proliferation of technology and increased ease of access to the Internet are facilitating cyber threats from a wide range of sources. From recreational hackers to organized terrorist organizations and legitimate nation states, the threats in cyberspace continue to increase and the points of origin are becoming more difficult to pin-point. The cyber attacks on Estonia and Georgia in 2007 and 2008, respectively, prove that cyberspace is a legitimate warfighting domain. Informed by these attacks, the 2009 Quadrennial Roles and Missions Review report identified cyberspace as one of four focus areas for the Department of Defense (DoD), and the armed services are moving quickly to address cyber personnel, training, equipment, and command and control issues. Currently, U.S. Strategic Command (USSTRACOM) is the department's "cyber command" and is responsible for operating, maintaining, protecting and monitoring the Global Information Grid (GIG) and, through the Defense Information Systems Agency's (DISA)Joint Task Force – Global Network Operations (JTF-GNO), exercises assured system and network availability, information protection, and information delivery for the DoD. At the operational level, DISA supports the Geographic Combatant Commanders (CCDRs) with remote field offices within each of their headquarters and Theater Network Operations Centers (TNCs) are collocated within most of the COCOM J6 organizations. Despite these support agencies, the CCDR does not have cyber resources at his immediate discretion as USSTRATCOM retains operational control of all units. In order to effectively address threats in the cyber domain, Geographic Combatant Commanders should establish a Joint Interagency Coordination Group – Cyber (JIACG-C) empowered to leverage joint, interagency, and civilian agency resources to support the commander's objectives. This paper will focus on this recommendation, analyzing the possible JIACG-C composition, staff functions, and command and control arrangements.

15. SUBJECT TERMS
Cyberspace, Combatant Commander, Joint Interagency Coordination Group, U.S. Strategic Command (USSTRATCOM), Joint Task Force – Global Network Operations (JTF-GNO)

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		27	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

JOINT INTERAGENCY COORDINATION GROUP – CYBER: EMPOWERING THE COMBATANT COMMANDERS AGAINST THE NO-BORDERS THREAT

by

OSVALDO ORTIZ

Major / U.S. Army

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: _____

04 May 2009

Contents

Abstract

The worldwide proliferation of technology and increased ease of access to the Internet are facilitating cyber threats from a wide range of sources. From recreational hackers to organized terrorist organizations and legitimate nation states, the threats in cyberspace continue to increase and the points of origin are becoming more difficult to pin-point. The cyber attacks on Estonia and Georgia in 2007 and 2008, respectively, prove that cyberspace is a legitimate warfighting domain. Informed by these attacks, the 2009 Quadrennial Roles and Missions Review report identified cyberspace as one of four focus areas for the Department of Defense (DoD), and the armed services are moving quickly to address cyber personnel, training, equipment, and command and control issues. Currently, U.S. Strategic Command (USSTRACOM) is the department's "cyber command" and is responsible for operating, maintaining, protecting and monitoring the Global Information Grid (GIG) and, through the Defense Information Systems Agency's (DISA) Joint Task Force – Global Network Operations (JTF-GNO), exercises assured system and network availability, information protection, and information delivery for the DoD. At the operational level, DISA supports the Geographic Combatant Commanders (CCDRs) with remote field offices within each of their headquarters and Theater Network Operations Centers (TNCs) are collocated within most of the COCOM J6 organizations. Despite these support agencies, the CCDR does not have cyber resources at his immediate discretion as USSTRATCOM retains operational control of all units. In order to effectively address threats in the cyber domain, Geographic Combatant Commanders should establish a Joint Interagency Coordination Group – Cyber (JIACG-C) empowered to leverage joint, interagency, and civilian agency resources to support the commander's objectives. This paper will focus on this recommendation, analyzing the possible JIACG-C composition, staff functions, and command and control arrangements.

INTRODUCTION

The mass proliferation of information technology around the world has created an unprecedented dependency on the Internet, wireless technology, cellular phones, computers, and networks. This is the influence of cyberspace. From online banking and instant messaging, to secure airborne video teleconferencing and flying unmanned aerial vehicles in Iraq from operation centers in the Pentagon, they are all cyberspace-enabled capabilities. The borderless reality of cyberspace has propagated to all "Levels of War"[1] and is now a significant planning consideration for commanders. When forces deployed in support of Operation IRAQI FREEDOM in 2003, for example, they used 50 times more bandwidth per person than during Operation DESERT STORM.[2] That is a significant increase and burden on limited telecommunications infrastructure. The demand for cyberspace-enabled services from the military force is high and continues to grow.

This increased reliance on cyberspace, however, has generated new challenges. The growing connectivity between military and other government and private sector information systems to the Internet is creating opportunities for attackers wishing to disrupt critical services and operations, as well as damage critical infrastructure.[3] These attackers range from recreational hackers to terrorist organizations, all capable of inflicting damage with a single computer, a modem connection, and easily available malware. In 2000 a single hacker unleashed the "I Love You" virus, infected over one million computers worldwide in less than five hours, and created an estimated $10 billion in damages and lost productivity.[4] The

[1] Milan N. Vego, *Joint Operational Warfare: Theory and* Practice (Newport, RI: Naval War College, 2007), IV-3.
[2] U.S. Army Training and Doctrine Command, *Cyber Operations and Cyber Terrorism*, Handbook No. 1.02 (12 August 2005), IV-1.
[3] U.S. Congress, Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community: Hearing on the Threats to the Nation*, 111th Cong. (12 February 2009).
[4] Mark Sauter and James Carafano, *Homeland Security: A Complete Guide to Understanding and Preventing Terrorism* (New York: The Heritage Foundation, 2005), 192.

cyber attacks on Estonia and Georgia in 2007 and 2008, respectively, also show that cyberspace can be a legitimate warfighting domain.

Discussing the need to organize the military for cyberspace operations, Chairman of the Joint Chiefs of Staff Admiral Michael Mullen simply stated, "We've got some significant challenges."[5] The Department of Defense (DoD) recognized the validity of this statement. In its 2009 Quadrennial Roles and Missions Review report, it identified cyberspace as one of four major focus areas.[6] The armed services followed suite and are now moving quickly to address cyber personnel, training, equipment, and command and control issues.

The biggest challenge is the command and control of the growing cyber force community. U.S. Strategic Command (USSTRATCOM) is the DoD's "global warfighter for cyberspace"[7] and is responsible for operating and defending the Global Information Grid (GIG).[8] Through its functional components Joint Functional Component Command for Network Warfare (JFCC-NW) and Joint Task Force – Global Network Operations (JTF-GNO), USSTRATCOM unilaterally deals with the challenges that lie within the cyber domain and maintains DoD's freedom of action in cyberspace. JTF-GNO specifically assures Global Information Superiority by providing "assured system and network availability, assured information protection, and assured information delivery."[9]

---

[5] Christopher J. Castelli, "Top brass launch manpower study for cyberspace operations," *Inside the Pentagon*, (5 March 2009), http://www.insidedefense.com/ (accessed 9 March 2009).
[6] Secretary of Defense. The Quadrennial Roles and Mission (QRM) Review Report, (Washington, DC: SECDEF, January 2009), 9.
[7] Commander, U.S. Strategic Command, "Statement of General Kevin P. Chilton before the Strategic Forces Subcommittee House Committee on Armed Services on the United States Strategic Command," 17 March 2009, 11.
[8] The GIG is defined in JP 3-13, page GL-8, as the 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. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services National Security Systems.
[9] U.S. Strategic Command, "Joint Task Force – Global Network Operations Fact Sheet," January 2009, http://www.stratcom.mil/factsheets/gno/ (accessed 7 March 2009).

At the operational level, the Defense Information Systems Agency (DISA), currently under the direction of Lt. Gen. Carroll F. Pollett,[10] supports every Geographic Combatant Commander (CCDR) with a remote field office (e.g. DISA CENT, DISA EUROPE). DISA's Theater Network Operations Center (TNC) is also collocated within most of the Combatant Command J6 organizations. Despite these embedded support agencies, in the event of a computer network attack[11] (CNA) or computer network defense[12] (CND) incident, the CCDRs do not have cyber resources at their immediate discretion. CDRUSSTRATCOM retains all operational control over assets and response.[13]

In order to effectively address threats in the cyber domain, Geographic Combatant Commanders should establish a Joint Interagency Coordination Group – Cyber (JIACG-C) empowered to leverage joint, interagency, and civilian agency resources to support the commander's objectives. Incorporating some elements of an Information Operations (IO) Cell and a conventional JIACG,[14] this new group will be empowered to leverage joint, interagency, and civilian agency resources to advise the CCDR and support his or her objectives. To set the stage, a brief review of the growth of the cyberspace is included here followed by a summary of its current posture in terms of influence, doctrine, definitions and DoD and service initiatives. The last item covered in the background section will be a brief review of some of the cyberspace threats and list recent examples of cyber attacks.

[10] In 2004, the Secretary of Defense designated the Director, DISA, as the Commander for JTF-GNO
[11] CNA is defined in JP 3-13 as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves," GL-5.
[12] CND is defined in JP 3-13 as "actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks," GL-5.
[13] Chairman, U.S. Joint Chiefs of Staff Instruction (CJCSI) 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND)*, (Washington, DC: CJCS, 12 August 2007), GL-7.
[14] As defined in Joint Publications 3-13 and 3-08, respectively.

The remaining sections will discuss the staff composition, functions, and command and control arrangements of the JIACG-C, scrutinize the feasibility of this new organization when compared to what U.S. Strategic Command already provides, and conclude with a summary of the proposed recommendation.

BACKGROUND: The Emergence of Cyberspace

Categorized as USSTRATCOM's "least mature mission area,"[15] cyberspace is a relatively new domain and operations, procedures and regulations are still under development. However, like the emergence of sea power in the late 1800s and air superiority in the 1900s, mastery of cyberspace is primed to be a dominant warfighting concern in the 21st century.

For brevity purposes, the following conclusion is acknowledged: cyberspace rose to prominence in the late 1990s with the fast expansion of the Internet. Vast awareness of cyberspace's capabilities and, more importantly, the vulnerabilities it facilitated and the potential for cyber attacks came to light at the end of the 20th century with the Year 2000 "millennium bug." While reports vary, it is estimated that the U.S. government spent more than $100 billion to "identify, test, and correct" hardware and software problems throughout its systems.[16] Numbers aside, the sheer amount of effort spent correcting this "bug," compounded by the massive media coverage made cyberspace front page news.

The Department of Defense, however, has taken precautionary measures to prepare its networks against attacks for some time. In 1997, the Joint Chiefs of Staff sponsored

[15] Matthew Hansen, "Cyberterrorism Fighters to brainstorm in Omaha," *Omaha-World-Herald*, 5 April 2009, http://www.omaha.com/ (accessed 6 April 2009).
[16] Erich Luening, "Report: U.S. to spend $100 billion fighting Y2K," *CNET News*, 17 November 1999, http://news.cnet.com/Report-U.S.-to-spend-100-billion-fighting-Y2K/2100-1091_3-233148.html (accessed 7 March 2009).

Exercise ELIGIBLE RECEIVER in which a 35-person hacker team disabled key command and control systems.[17] In 2000, JTF-Computer Network Operations command was created, and, in 2002, the Naval War College simulated a series of cyber attacks on key infrastructures.[18] Despite the growing reliance on digital technology, these and other initiatives have postured DoD defenses to a level that has thus far prevented major effects from cyber attacks. While specific threats will be mentioned in a later section, the emergence of cyberspace has not gone unnoticed by, among others, terrorist organizations. Several major terrorist groups, including Al Qaeda, HAMAS, and the Revolutionary Armed Forces of Columbia (FARC) now use the Internet to recruit personnel and distribute messages.[19]

BACKGROUND: Cyberspace Now

Computer networks and their associated sensors and communications links will emerge, if they have not already emerged, as potential centers of gravity at all levels of war.
- Milan N. Vego
Joint Operational Warfare: Theory and Practice

Today, all doctrinal operational functions rely on cyberspace. For movement and maneuver, Blue Force Tracker is a critical situational awareness tool in Iraq and Afghanistan. In command and control (C2), Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems are a complex mix of radios, radars and computers. And for Fires and Logistics, the F-35 weapon system[20] and self-reporting maritime Automatic Identification System (AIS) use state-of-the-art information

[17] Russell D. Howard, James J. F. Forest, and Joanne C. Moore, *Homeland Security and Terrorism: Readings and Interpretations* (New York: McGraw-Hill Professional, 2005), 167-168.
[18] John Rollins and Clay Wilson, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, CRS Report RL33123, (Washington, DC: Congressional Research Service, 22 January 2007), 10.
[19] Howard, Forest, and Moore, *Homeland Security and Terrorism*, 170.
[20] Siobhan Gorman, August Cole and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, 21 April 2009, http://online.wsj.com/article/SB124027491029837401.html (accessed 21 April 2009).

technology. Joint Task Force headquarters now operate with near-real time information and maintain up-to-the-minute common operating pictures facilitated by commercial-off-the-shelf and voice over Internet protocol (VOIP) technology. By comparison, a general service (GENSER) message that took more than an hour to process during Operation DESERT STORM takes less than a second today.[21] Figure 1 is a graphical depiction of cyberspace's influence in the operational environment now. It accurately depicts the core, supporting and related capabilities of information operations as outlined in Joint Publication 3-13, *Information Operations*, and, unlike many of the current official publications, specifically includes cyberspace as an operating domain. Refer to Appendix B for a listing of all abbreviations used in this figure (and paper).

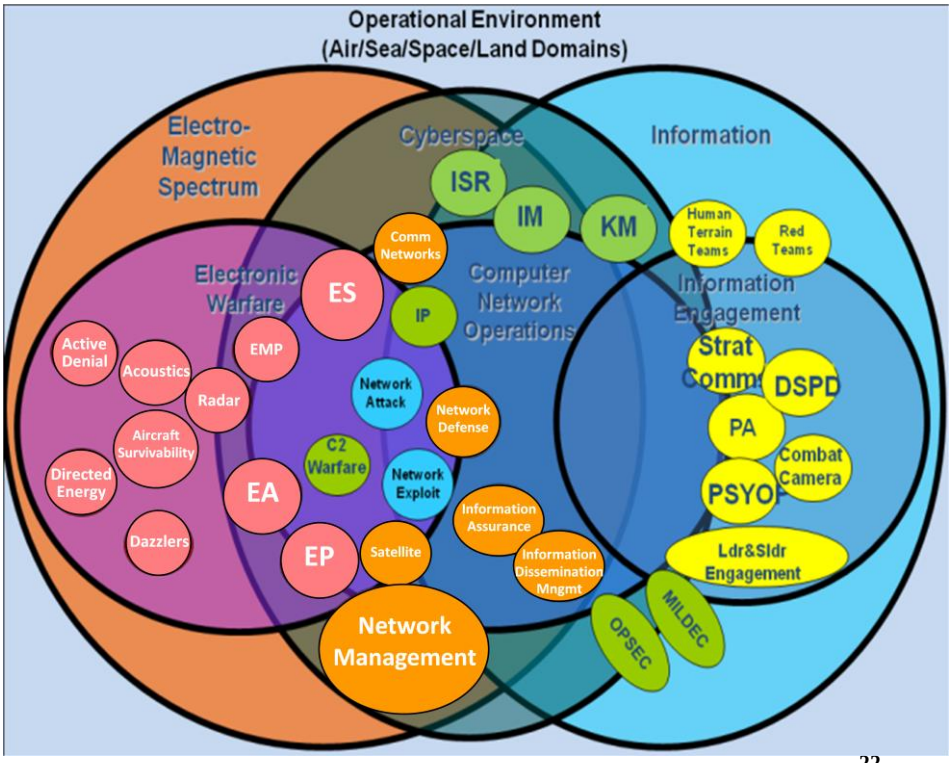


Figure 1: Cyberspace's Relation to the Operational Environment[22]

[21] Vego, *Joint Operational Warfare*, III-69.
[22] Fred Harper, "U.S. Army Computer Network Operations-Electronic Warfare Proponent," Powerpoint, Ft. Leavenworth, KS: U.S. Army Combined Arms Center, http://usacac.army.mil/cac2/ew/ (accessed 3 April 2009).

Cyberspace is a priority at all levels of government. The President George W. Bush administration introduced the *National Strategy to Secure Cyberspace* in 2003 and, in 2008, the *Comprehensive National Cybersecurity Initiative* (CNCI) which aimed to establish federal cyber security and monitoring guidelines.[23] In February 2009, President Barack Obama directed the "immediate review of the plan, programs, and activities underway throughout the government dedicated to cyber security."[24]

The Secretary of Defense in 2006 also signed the *National Military Strategy for Cyberspace Operations* (NMS-CO) and formally defined cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." [25] Beyond definitions, the NMS-CO offers a "comprehensive military strategy for DOD to enhance U.S. military strategic superiority in cyberspace."[26] Finally, a recent memorandum from the Vice Chairman of the Joint Chiefs of Staff specifically defined cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[27]

The combination of all these documents is guiding DoD cyber efforts. New organizations like Air Force Cyber Command (AFCYBER), Naval Network Warfare

[23] John Rollins and Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, CRS Report R40427, (Washington, DC: Congressional Research Service, 10 March 2009), 1.
[24] Melissa Hathaway was named the Acting Senior Director for Cyberspace for the National Security and Homeland Security Council on 9 February, 2009, and placed in charge of this 60-day interagency review.
[25] Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, (Washington, DC: CJCS, December 2006), 3.
[26] Chairman, U.S. Joint Chiefs of Staff, *Homeland Defense*, Joint Publications (JP) 3-27 (Washington, DC: CJCS, 12 July 2007), VII-8.
[27] Gen James E. Cartwright, VCJCS, for Deputy Secretary of Defense. Action Memorandum, 29 September 2008.

Command (NETWARCOM), and the Army's Network Warfare Battalion (ANWB) are pressing with the development of doctrine, equipment, and the force's new "cyber warrior."

BACKGROUND: Cyberspace Threats

[Cyber security] is a strategic issue on par with weapons of mass destruction and global jihad.

- Center of Strategic and International Studies
Securing Cyberspace for the 44th Presidency

Already briefly mentioned, there are a growing number of cyber attack sources that include recreational hackers, terrorist groups, transnational actors and even nation-states.[28] Table 1 on the next page lists several recent CNA attacks. The NMS-CO also specifically identified the six categories of cyberspace threats as traditional, irregular, catastrophic, disruptive, natural and accidental.[29] Because of this wide range of threats and the length limitations of this paper, only CND and CNAs, two of three core capabilities of computer network operations (CNO), are discussed henceforth.

"America is under widespread attack in cyberspace," was the statement of former USSTRATCOM commander General James E. Cartwright to Congress in March 2007.[30] These CNA examples undoubtedly prove the capability to cause harm through cyberspace is real and that we must prepare accordingly. Beyond user inconvenience and denial of Internet service, CNAs pose a threat to national security, if the right computer is hacked, to every day operations, if baking systems are shut down, or to American lives, if an air control tower is disabled. The following sections focus on the recommendation of a Joint Interagency Coordination Group – Cyber (JIACG-C) for every Combatant Commander (CCDR). The command and control of cyber forces will not be discussed; instead, this paper addresses the need of the CCDRs to have their own resources to prepare for CND/CNAs and accomplish

[28] Henry S. Kenyon, "Strategic Command Directs Cyber Operations," *Signal*, July 2008, 29.
[29] Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, C-1.
[30] John J. Tkacik, Jr, *Trojan Dragons: China's International Cyber Warriors*, The Heritage Foundation No. 1735 (Washington, DC: The Heritage Foundation, 12 December 2007), 1.

the vision of the NMS-CO of informed, unified action through industry, interagency and coalition cooperation against cyberspace threats.

2006: a computer attack against the U.S. Naval War College forces officials to disconnect the entire college from the Internet.[31]
2007: Estonia is subjected to a massive cyber-attack that brings down the web sites of several media organizations, the Estonian parliament, and forces Estonia's largest bank to shut down its online banking network for a short time. The financial impact is unclear but estimates start at $1 million.[32] The attack came after Estonia removed a Russian World War II memorial from Talinn.
2008: a coordinated denial-of-service attack hits the Georgian government, incidentally coinciding with Russian ground attacks, and disables most of its information infrastructure including several government web sites.[33] The attack disrupted government operations and hindered civil-military coordination in the midst of the Russian attack.
2009: Chinese computer system "GhostNet" infiltrates over 1,300 computers in the United States and more than 100 other countries.[34]
April 2009: during a cyberspace conference, military officials disclose that the Pentagon spent more than $100 million in the last six months responding to and repairing damage from cyber attacks.[35]

Table 1: Examples of recent CNA attacks

RECOMMENDATION: JOINT INTERAGENCY COORDINATION GROUP – CYBER

The concept of a Joint Interagency Coordination Group is not new. Joint Publication 3-08 already defines a JIACG as "an interagency staff group that establishes regular, timely, and collaborative working relationships between civilian and military operational planners,"[36] and U.S. Joint Forces Command (USJFCOM) experimented with the concept of placing a civilian-oriented interagency element on combatant commander staffs[37] before U.S.

[31] Associated Press, "Hacker Attack U.S. Naval War College," *MSNBC*, 5 December 2006, http://www.msnbc.msn.com/id/16057306/ (accessed 7 April 2009).
[32] Mark Landler and John Markoff, "Digital fears emerge after data siege in Estonia," *New York Times*, 29 May 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html (accessed 4 April 2009).
[33] Hansen, "Cyberterrorism Fighters to brainstorm in Omaha," (accessed 6 April 2009).
[34] Ibid
[35] Lolita C. Baldor, "Pentagon spends $100 million to fix cyber attacks," *The Associated Press*, 7 April 2009, http://www.google.com/hostednews/ap/article/ALeqM5i-l6vKmsnP1XSIDouvQ2hcc2mNTAD97DPBPO0/ (accessed 7 April 2009).
[36] Chairman, U.S. Joint Chiefs of Staff, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I*, Joint Publications (JP) 3-08 (Washington, DC: CJCS, 17 March 2006), II-14.
[37] U.S. Joint Forces Command, "Joint Interagency Coordination Group," http://www.jfcom.mil/about/fact_jiacg.htm (accessed 02 April 2009).

Southern Command (USSOUTHCOM) restructured its staff in 2006. Specific to cyberspace, the Department of Homeland Defense's (DHS) National Cyber Response Coordination Group (NCRCG) was established in 2003 and is the "principal interagency mechanism for managing cyberspace incidents of national significance."[38] This group facilitates the federal coordination of response activities of all the departments that compromise the NCRCG, including the DoD.

Proving the value of interagency coordination, United States Northern Command utilized its NORAD-USNORTHCOM Interagency Coordination (N-NC IC) group to synchronize interagency activities in areas impacted by Hurricane Katrina in 2005 and the California wildfires of 2008. N-NC IC also responded to several other assistance requests generated by the National Response Plan framework.[39] USSOUTHCOM's Joint Interagency Task Force – South, comprised of DoD, law enforcement organizations, intelligence agencies and international partners, interdicted more than 500 metric tons of cocaine between 2006 and 2008.[40]

So, what is the current CCDR's staff "cyber" shortfall? Why a JIACG-C? In short, there are entirely too many elements involved in the CNA and CND umbrella of the CCDR. For starters, the CNA warfighting functions normally reside in the J3 directorate, or equivalent, of the COCOM staff. The staff of the Information Operations Cell Chief, for example, is normally designated as the J-39. CND, on the other hand, falls under the auspices of the J6 and its system administrators, Designated Approving Authorities (DAA), Information Assurance Management (IAMO) and Information Assurance Security (IASO)

[38] Chairman, U.S. Joint Chiefs of Staff, *Homeland Defense*, Joint Publications (JP) 3-27, VII-6.

[39] Bob Felderman, "NORAD-USNORTHCOM Operations Plan Summary," Powerpoint, www.roa.org/site/DocServer/20080930_Felderman_N-NC_Plans_Summary_Interagency.ppt?docID=14701 (accessed 27 April 2009).

[40] U.S. Southern Command, "Command Briefing," Powerpoint, www.southcom.mil (accessed 5 September 2008).

Officers. The call for a JIACG-C does not imply that USSTRATCOM and JTF-GNO are not supporting the CCDR. However, the current operational control (OPCON) and tactical control (TACON) relationships between the multiple commands described in the introduction and the disjointed J3-J6 cyber efforts are not optimal in terms of unity of command arrangements. Further complicating matters are the elements of the Theater Network Operations Control Centers (TNCC) and service Geographic Network Operations Centers (GNOSC). As an example, Appendix A depicts the command relationships of the U.S Army's Network Enterprise Technology Command (NETCOM). Because of the source material, a diagram of JTF-GNO's subordinate is not included but can be reviewed in JTF-GNO's secure web page.[41]

Unfortunately, the virtual, fast-paced reality of cyberspace demands that the commander have a complete understanding of the threats in this new domain at all times and that he have it as rapidly and in as easily accessible a manner as possible. The concept discussed here is therefore to surround commanders with the right set of tools, in this case, civilian and military subject matter experts (SMEs), so they can plan and prepare CND as well as react to CNAs. Bottom line, the vision of this recommendation is to provide the CCDRs with the least complex C2 arrangements connected to their own band of cyber experts which would be under their direct operational, tactical and administrative control.

JIACG-C STAFF COMPOSITION

The ideal composition of a JIACG-C will be a combination of an IO Cell and a conventional JIACG. Refer to Figure 2 for the doctrinal depiction of both of these concepts.

[41] The command relationship between JTG-GNO and its operations centers is not classified. However, no open-source references were found, except the *Joint Concept of Operations for Global Information Grid NetOps* under the JTF-GNO SIPRNET web page at http://jtfgno.smil.mil/site/documents/netopsconops/ (accessed 11 March 2009).

The staff of a JIACG-C must include members of the CCDR's staff that already share knowledge about the commander's mission, available facilities and resources, and the operational restraints and constraints within the command and geographic area of operations. More importantly, the group must also understand the most likely threats within their areas of operation. For example, USAFRICOM is responsible for areas that are not as industrially advanced as those in USEUCOM; the possible sources of cyber threats could therefore be more limited. In short, members of the JIACG-C must have local situational awareness.

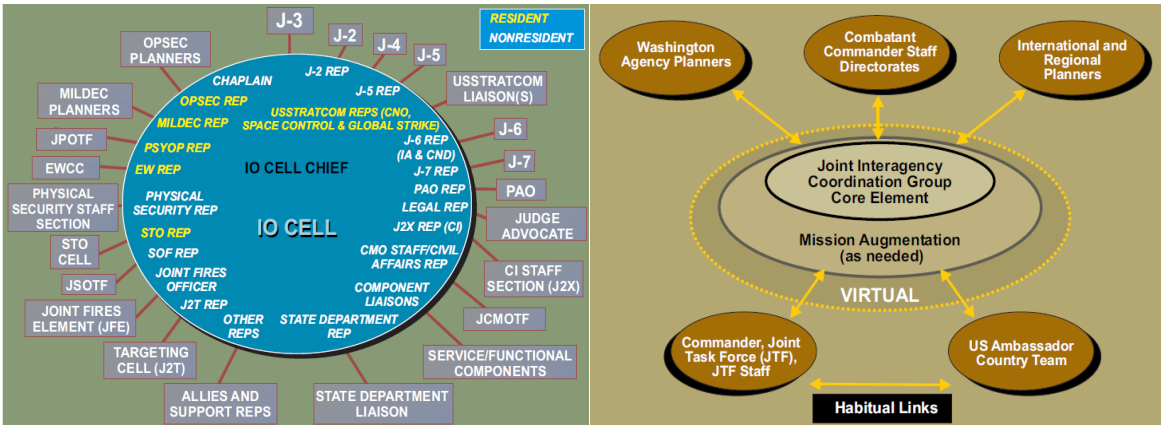


Figure 2: Notional Information Operations and JIACG Structures (*reprinted from JP 3-13 and JP 3-08, respectively*)

Second, each JIACG-C must be composed of government, interagency, and civilian or private sector SMEs. This is a restatement of multiple studies and reports for the increased cooperation between the agencies.[42] Specialized cyber training is essential to the success of this group. While it is fruitless to list specific training qualifications and sources,

[42] Report of the CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, 48. "The goal is a trusted and operationally focused collaborative alliance among the government, academia, and the private sector." Leigh Armistead, ed., *Information Operations: Warfare and the hard reality of soft power* (Washington, D.C: Potomac Books, 2004), 162. "The need for increased integration and cooperation among the diverse members of the interagency community, as well as the private sector, academia, and others, will eventually force those within the DoD to come to terms with the limitations imposed by traditional military planning methods and procedures." Martin N. Wybourne, Martha F. Austin, Charles C. Palmer. *Report to the Chairman and Ranking Member of the US Senate Committee on Homeland Security and Government Affairs: National Cyber Security* (Washington, DC, 2009), 4. "A coordinated and collaborative approach is needed."

there needs to be some commonality in regards to the level of understanding on subjects such as cyber forensics or for the group members to be Certified CISCO Network Administrators (CCNA) or graduates of the Army's Electronic Warfare course at Fort Sill, OK.

While the exact membership will likely vary from COCOM to COCOM, each group should have the following core staffing and/or capabilities:

J2: Intelligence and cyber threat assessment	Department of Justice Rep: Familiar with the local, national and international cyber laws
J6: Computer Network Operations and liaison to JTF-GNO	Department of State: Regional Information/Computer Operations expert
J3: Current Operations Rep	Private Sector/Civilian: cyber/CNA SME
J5 Future Operations Rep	Private Sector/Civilian: cyber/CND SME

Table 2: Proposed JIACG-C

There are obviously a number of other details that need to be addressed including where the above listed personnel will come from. There are a limited resources available to the commander. But a key takeaway is that a JIACG-C is not intended to be as large as an IO Cell and that it incorporates some of the virtual elements of the notional JIACG into its core staff.

JIACG-C STAFF FUNCTIONS

The primary function of the JIACG-C, as already stated, is to leverage joint, interagency, and civilian agency resources to properly advise the CCDR of cyber threats. Moreover, the group will have situational awareness of the CNA and CND capabilities and limitations at the commander's disposal as well as an understanding of the prevalent vulnerabilities in the geographic area of responsibility. Additional functions of the JIACG-C can include:

- Conduct CNA/CND deliberate and crisis action planning.

- Develop a continuity of operations plan that includes the restoral of services, operation through degradation, and transition of responsibilities in the event of a CNA.
- Research CND technology and coordinate with agencies as required for its implementation.
- Research and develop cyber rules of engagement as applicable to the CCDR area of responsibility and in conjunction with participating agencies.
- Provide civilian agency insight on cyber matters.
- Develop and implement a risk management program that includes security awareness training and risk mitigation measures.

This is certainly not an all-inclusive list, and several more details should be included. The overarching theme is the similarities to the functions of an IO Cell and notional JIACG as outlined in JP 3-13 and JP 3-08, respectively. It is also important to point out that these cyber warrior functions are not organic to the CCDRs, yet most are identified as "strategic imperatives" in the NMS-CO. [43]

JIACG-C STAFF COMMAND AND CONTROL RELATIONS

The United States can achieve superiority in cyberspace only if supported and supporting relationships are clearly defined and executed.
- The National Military Strategy for Cyberspace Operations

The intent of this paper is not to address the command and control of cyber warriors or of CND and the most-always classified CNA operations. JIACG-C is an advising council to the CCDR. However, as concluded in a recent report on cyber security, "organizations at

[43] Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, 10. "Strategic imperatives are those considerations that must be taken into account to operate successfully in the [cyberspace] domain."

all levels will need to accelerate decision-making if cyber defense is to be most effective."[44] Considering the time-space nature of cyberspace – near instant effects worldwide – effective C2 relations between CDRUSSTRATCOM and its subordinate commands, service-centric organizations, and the CCDRs and their JIACG-Cs will be critical to the synchronization of cyberspace operations. After all, as the 9/11 Commission Report indicated, competing command and control relations between first responders or, in this case, operational commanders will only hinder the response to the threat or attack.[45]

It is worth restating USSTRATCOM's current doctrinal responsibilities. They include the coordination and integration of all DoD information operations "to include planning, directing, and identifying desired characteristics and capabilities for DoD-wide CND; and identifying desired characteristics and capabilities of CNA, conducting CNA in support of assigned missions, and integrating CNA capabilities in support of other combatant commanders, as directed."[46] CDRUSSTRATCOM is most often the supported commander and, with the emergence of the Network Operations (NetOps)[47] concept and growing emphasis on cyber security, the projected responsibilities of the command are assured to increase.

The actual command and control of the JIACG-C within a COCOM staff will vary from command to command. In USSOUTHCOM, the group could fall under the "Security and Intelligence Directorate"; in USCENTCOM and USPACOM, the group could be under

---

[44] Report of the CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, 30.
[45] National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington, DC: W. W. Norton & Company, July 2004), 36, 298, 396
[46] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publications (JP) 3-13, IV-1.
[47] Chief Information Officer, Department of Defense, *NetOps Strategic Vision* (Washington, DC: SECDEF, December 2008), 1. Defines NetOps as "the DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG."

the supervision of the J6. Regardless of the staff hierarchy, the point is that the group is under the jurisdiction of CCDR.

STATUS QUO – USSTRATCOM

While there are benefits for a JIACG-C at every COCOM headquarters, there are some drawbacks to this recommendation. The first is the obvious dilution of an already limited population of resources. By spreading subject matter experts across six combatant commands, cyber expertise might end up too far spread across DoD, at least in the short term until more cyber warriors are processed through the service stovepipes, sourced from other government agencies or hired from the private sector. One can argue that the U.S. intelligence communities (i.e. the Federal Bureau of Investigation, Central Intelligence Agency and Office of the Director of National Intelligence) already suffer from this expertise dilution problem.

By keeping USSTRACOM as the lead agency for all cyber matters, the vision of a single, "robust National Cyber Security Center" recommended in a March 2009 Congressional Research Service report is certainly accomplished[48] at least at the DoD level. Furthermore, USSTRATCOM and JTF-GNO have the advantage of working the cyber mission for more than 11 years[49] and undoubtedly possess the domain expertise and capability for a rapid and aggressive response to the worst possible case CNAs, sometimes referred to as "Electronic Pearl Harbor", "Digital September 11" and "Cybergeddon."[50]

---

[48] Rollins and Henning, *Comprehensive National Cybersecurity Initiative*, CRS Report R40427, 16.
[49] Although JTF-GNO didn't realign under USSTRATCOM until 2004, its preceding command, JTF-CNO, was established in 1998.
[50] John Goetz, Marcel Rosenbach, and Alexander Szandar, "National Defense in Cyberspace," *Spiegel Online International*, 11 February 2009, http://www.spiegel.de/international/germany/0,1518,606987,00.html (accessed 17 March 2009).

Even if a recent report of the Secretary of Defense considering the creation of a new cyber sub-unified command is accurate,[51] the new organization will function under USSTRATCOM in the early stages until personnel and capabilities are transferred. The power to ensure the security and availability of the GIG will still rest in one command.

The problem with this organization approach, however, is that it does not place an emphasis on the combatant commands. Expertise must be forward in the theaters of operation and with the CCDRs because the nature of the cyber medium demands these organizations react and make decisions in a matter of minutes. While CDRUSSTRATCOM manages multiple resources and is empowered with a wide array of authorities, it is the individual CCDRs who are the subject matter experts in their area of operations. As for the limited pool of SMEs, efforts to expedite the training of personnel will need to be put in place by all the services. Moreover, training will need to be standardized at some level so that a cyber consultant at USPACOM, for example, possesses the same type of skills as one at USAFRICOM. Until the process is solidified, a transitional period of diluted expertise at the COCOMs will need to be bared and USSTRATCOM will continue to be the center of cyber excellence.

CONCLUSION

"The Department of Defense relies on cyberspace to achieve national military objectives in the areas of military, intelligence, and business operations."
- The National Military Strategy for Cyberspace Operations

Cyber security is now a major national security problem for the United States[52] and the Department of Defense and its operational level commanders must prepare accordingly. To use the words of Gen. Kevin P. Chilton, CDRUSSTRATCOM, there needs to be a shift

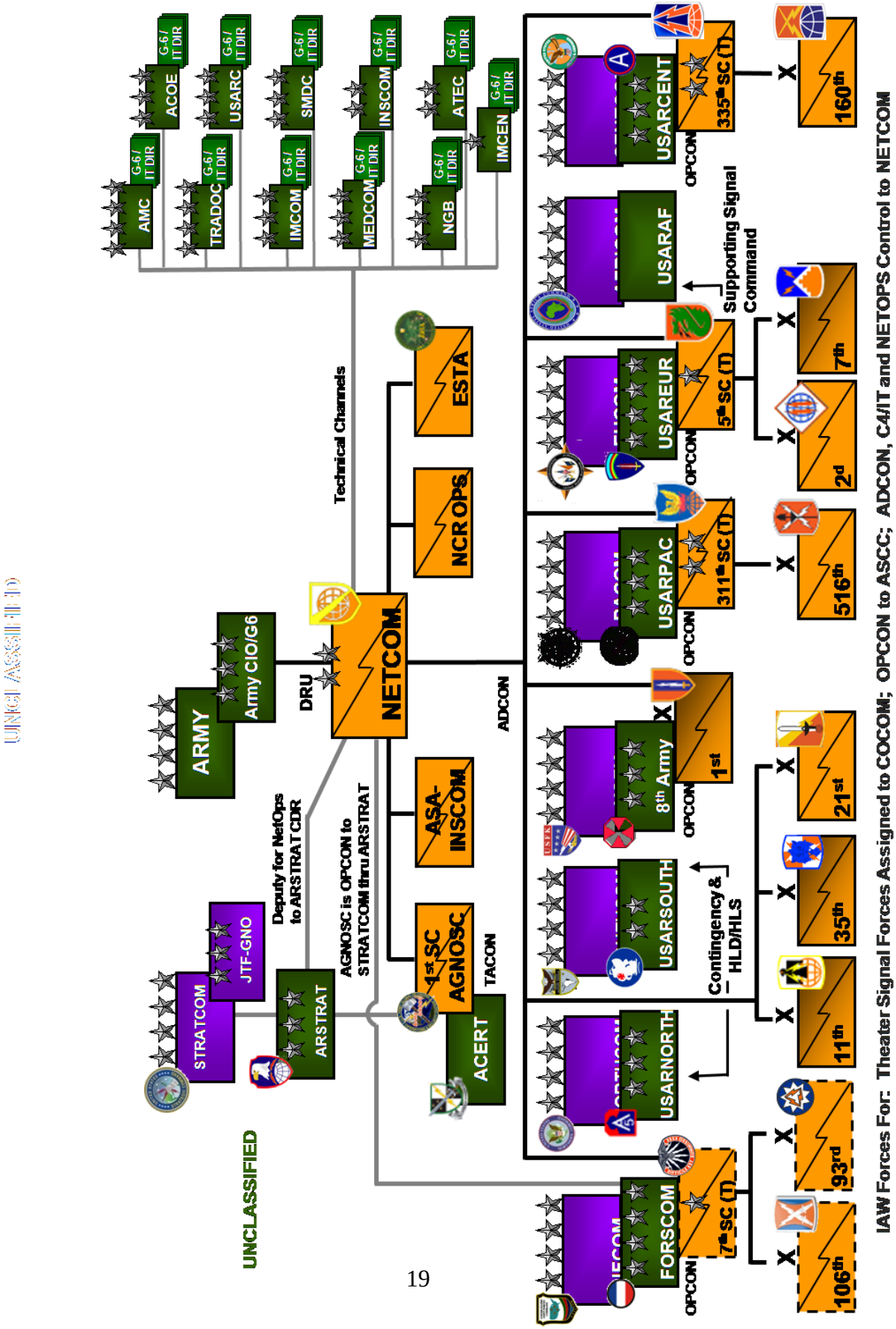
[51] Sebastian Sprenger, "Gates Weighs Creation of Cyberspace Command under STRATCOM," *Inside the Air Force*, 17 April 2009, http://www.insidedefense.com/ (accessed 17 April 2009).
[52] Report of the CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, 1.

from "watching and reacting" to "knowing and predicting"[53] the threats that lie within the cyber domain. The best way to execute this is by empowering each CCDR with a Joint Interagency Coordination Group – Cyber.

The JIACG-C integrates cyber subject matter experts in the CCDRs staff, encourages a coordinated and collaborative approach in planning and preparing for CNAs and CND, and heeds the call of the Secretary of Defense to effectively and efficiently structure forces and associated processes and procedures to execute DoD's priorities in cyberspace.[54] USSTRATCOM and JTF-GNO provide critical resources and capabilities but are too far removed from the specific concerns of the CCDRs. Empower the operational planners with the right set of capabilities, and they will assure the defense of cyberspace. Otherwise, the United States will be the next cyber victim – the next Georgia and Estonia.

[53] Commander, U.S. Strategic Command, "Statement of General Kevin P. Chilton," 10.
[54] Secretary of Defense. The Quadrennial Roles and Mission (QRM) Review Report, 14.

APPENDIX A: U.S. Army Network Enterprise Technology Command



APPENDIX B: Abbreviations

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCDR	Geographic Combatant Commander
CNA	Computer Network Attack
CND	Computer Network Defense
CNO	Computer Network Operations
DISA	Defense Information Systems Agency
DoD	Department of Defense
DSPD	Defense Support for Public Diplomacy
EA	Electronic Attack
ES	Electronic Surveillance
EP	Electronic Protection
GCC	Geographic Combatant Commander
GIG	Global Information Grid
IM	Information Management
IO	Information Operations
JIACG-C	Joint Interagency Coordination Group - Cyber
JFCC-NW	Joint Functional Component Command for Network Operations
JTF-GNO	Joint Task Force – Global Network Operations
KM	Knowledge Management
MILDEC	Military Deception
NMS-CO	National Military Strategy for Cyberspace Operations
OPSEC	Operations Security
PA	Public Affairs
PSYOP	Psychological Operations
TNC	Theater Network Operations
TNCC	Theater Network Operations Center
USSTRATCOM	United States Strategic Command

BIBLIOGRAPHY

Achterberg, Kevin L. "Cyberspace – A New Medium for Operational Warfare." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2003.

Anderson, Erin M. "Fact or Fiction: Internet Surveillance and Reconnaissance Cell." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008.

Armistead, Leigh, ed. *Information Operations: Warfare and the hard reality of soft power*. Washington, D.C: Potomac Books, 2004.

Associated Press. "Hacker Attack U.S. Naval War College." *MSNBC*, 5 December 2006. http://www.msnbc.msn.com/id/16057306/ (accessed 7 April 2009).

Baldor, Lolita C. "Pentagon spends $100 million to fix cyber attacks," *The Associated Press*, 7 April 2009. http://www.google.com/hostednews/ap/article/ALeqM5i-l6vKmsnP1XSIDouvQ2hcc2mNTAD97DPBPO0/ (accessed 7 April 2009).

Cartwright, Gen. James E. Office of the Vice Chairman of the Joint Chiefs of Staff for the Deputy Secretary of Defense. Action Memorandum, 29 September 2008.

Castelli, Christopher J. "Top brass launch manpower study for cyberspace operations," *Inside the Pentagon*, 5 March 2009. http://www.insidedefense.com/ (accessed 9 March 2009).

Commander, U.S. Strategic Command, "Statement of General Kevin P. Chilton before the Strategic Forces Subcommittee House Committee on Armed Services on the United States Strategic Command." 17 March 2009.

Elliot, Michael C. "Operational Command and Control of Joint Task Force Cyberspace Operations." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2008.

Felderman, Bob. "NORAD-USNORTHCOM Operations Plan Summary." Powerpoint. www.roa.org/site/DocServer/20080930_Felderman_N-NC_Plans_Summary_Interagency.ppt?docID=14701 (accessed 27 April 2009).

Goetz, John, Rosenbach, Marcel, and Szandar, Alexander. "National Defense in Cyberspace," *Spiegel Online International*, 11 February 2009. http://www.spiegel.de/international/germany/0,1518,606987,00.html (accessed 17 March 2009).

Gorman, Siobhan, Cole, August and Dreazen, Yochi. "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal,* 21 April 2009. http://online.wsj.com/article/SB124027491029837401.html (accessed 21 April 2009).

Hansen, Matthew. "Cyberterrorism Fighters to brainstorm in Omaha," *Omaha-World-Herald,* 5 April 2009. http://www.omaha.com/ (accessed 6 April 2009).

Harper, Fred. "U.S. Army Computer Network Operations-Electronic Warfare Proponent." Powerpoint. Ft. Leavenworth, KS: U.S. Army Combined Arms Center. http://usacac.army.mil/cac2/ew/ (accessed 3 April 2009).

Howard, Russell D., Forest, James J. F., and Moore, Joanne C. *Homeland Security and Terrorism: Readings and Interpretations*. New York: McGraw-Hill Professional, 2005.

Johns, Raymond and Hanessian, Bruce. "Domain Expertise and Command and Control," *Joint Forces Quarterly,* no. 49 *(2nd quarter 2008)*: 48.

Kenyon, Henry S., "Strategic Command Directs Cyber Operations," *Signal*, July 2008.

Landler, Mark and Markoff, John. "Digital fears emerge after data siege in Estonia," *New York Times,* 29 May 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html (accessed 4 April 2009).

Luening, Erich. "Report: U.S. to spend $100 billion fighting Y2K," *CNET News*, 17 November 1999. http://news.cnet.com/Report-U.S.-to-spend-100-billion-fighting-Y2K/2100-1091_3-233148.html (accessed 7 March 2009).

National Commission on Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington, DC: W. W. Norton & Company, July 2004.

Report of the CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*. Washington, DC: Center of Strategic and International Studies, 2008.

Rollins, John and Henning, Anna C. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations,* CRS Report R40427. Washington, DC: Congressional Research Service, 10 March 2009.

Rollins, John and Wilson, Clay. *Terrorist Capabilities for Cyberattack: Overview and Policy Issues,* CRS Report RL33123. Washington, DC: Congressional Research Service, 22 January 2007.

Sauter, Mark and Carafano, James. *Homeland Security: A Complete Guide to Understanding and Preventing Terrorism.* New York: The Heritage Foundation, 2005: 192.

Souder, Jeffrey K. "Space, Time and Force: Relationships in Cyber Space." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2001.

Sprenger, Sebastian. "Gates Weighs Creation of Cyberspace Command under STRATCOM," *Inside the Air Force,* 17 April 2009. http://www.insidedefense.com/ (accessed 17 April 2009).

Tkacik, John J. Jr. *Trojan Dragons: China's International Cyber Warriors*, The Heritage Foundation No. 1735. Washington, DC: The Heritage Foundation, 12 December 2007.

U.S. Army Training and Doctrine Command, *Cyber Operations and Cyber Terrorism*, Handbook No. 1.02. 12 August 2005.

U.S. Congress, Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community: Hearing on the Threats to the Nation*, 111th Cong. 12 February 2009.

U.S. Joint Forces Command. "Joint Interagency Coordination Group." http://www.jfcom.mil/about/fact_jiacg.htm (accessed 02 April 2009).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Homeland Defense*. Joint Publications (JP) 3-27. Washington, DC: CJCS, 12 July 2007.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publications (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations Vol I*. Joint Publications (JP) 3-08. Washington, DC: CJCS, 17 March 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. Washington, DC: CJCS, December 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Assurance (IA) and Computer Network Defense (CND)*. U.S. Joint Chiefs of Staff Instruction (CJCSI) 6510.01E. Washington, DC: CJCS, 12 August 2007

U.S. Office of the Secretary of Defense. *The Quadrennial Roles and Mission (QRM) Review Report*. Washington, DC: SECDEF, January 2009.

U.S Office of the Secretary of Defense Chief Information Officer. *NetOps Strategic Vision*. Washington, DC: SECDEF, December 2008.

U.S. Southern Command. "Command Briefing." Powerpoint, www.southcom.mil (accessed 5 September 2008).

U.S. Strategic Command. "Joint Task Force – Global Network Operations Fact Sheet." January 2009. http://www.stratcom.mil/factsheets/gno/ (accessed 7 March 2009).

Vego, Milan N. *Joint Operational Warfare: Theory and* Practice. Newport, RI: Naval War College, 2007.

Wybourne, Martin N., Austin, Martha F., Palmer, Charles C. *Report to the Chairman and Ranking Member of the US Senate Committee on Homeland Security and Government Affairs: National Cyber Security*. Washington, DC, 2009.