



Ike Skelton Library

<http://www.jfsc.ndu.edu/library/default.asp>

757-443-6401 (DSN 646-6401)

Cyber Security

Pathfinder ☀ April 2010

“The basic message is simple: Cyberspace is its own medium with its own rules. Cyberattacks, for instance, are enabled not through the generation of force but by the exploitation of the enemy’s vulnerabilities. Permanent effects are hard to produce. The medium is fraught with ambiguities about who attacked and why, about what they achieved and whether they can do so again. Something that works today may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace. Such tenets must be rethought.”

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Arlington, VA: RAND, 2009.

<http://www.rand.org/pubs/monographs/MG877/>

RECOMMENDED RESOURCES & SEARCH TERMS

SUBSCRIPTION DATABASES ARE ONLY ACCESSIBLE THROUGH BLACKBOARD, UNDER IKE SKELTON LIBRARY, “ONLINE RESEARCH” ; OR UNDER “LIBRARY RESOURCES” ON THE JFSC INTRANET AND ON LIBRARY COMPUTER DESKTOPS.

Recommended search terms: **Search terms can be combined to focus/narrow a search and remember to look for ways to limit searches by date, or for ‘advanced search’ features. (Some tutorials are available on BlackBoard: Online Research, under the link to that particular database.)*

<u>Search Terms</u>	<u>Internet Resources</u>	<u>Subscription databases</u>
<ul style="list-style-type: none"> • Cyber Security • Cyber Attacks • Cyber Warfare • Network Centric Warfare (NCW) • Cyber Defenses 	<ul style="list-style-type: none"> • Defense Technical Information Center DTIC www.dtic.mil • CIAO www.ciao.org • Government Google www.google.com/unclesam • Homeland Security Digital Library www.hsdl.org 	<ul style="list-style-type: none"> • ProQuest • Praeger International • PolicyFile • Ike Skelton Library Catalog

Other Associated Terms

Cyberterrorism; Internet Attacks; Internet Defenses; Information Technology Infrastructure; Information Warfare; Computer Network Operations; CNO (Computer Network Operations); Cyber Threats; Critical Information Infrastructure; Cyber-Vision; Cyber Force Development; Cyberspace; Russian Federation; NATO Center Of Excellence For Cyber Defense; Former Soviet Satellites; OSCE (Organization For Security And Cooperation In Europe); People’s Republic of China; GIG (Global Information Grid); CAN (Computer Network Attack); USCYBERCOM (U.S. Cyber Command)

IKE SKELTON LIBRARY CATALOG

Search Keywords: Cyberterrorism, Information Warfare, Cyber Threats, Cyber Security, Cyber Terrorism

Books & Documents

(Listed by call number)

Call No. HV 6773 .C64 2006

Colarik, Andrew M. *Cyber Terrorism : Political and Economic Implications*. Hershey, PA: Idea Group, 2006.

Focus: "The power of terrorism; Cyber terrorism evolution; Global information infrastructure; Current cyber attack methods; Attack scenarios; Thoughts for the future."

Call No. U 163 .C38 2009

Caulkins, Bruce D. *Proactive Self-Defense in Cyberspace*. Arlington, VA : Institute of Land Warfare, Association of the United States Army, 2009.

Focus: "This paper discusses the security vulnerabilities of websites and computer networks and how they have been and can be exploited, and offers solutions that the Department of Defense can implement to protect itself against a cyber attack. According to the author, DoD's cyber defense strategy must be proactive, dynamic and polymorphic in nature to anticipate future attacks. The strategy requires personnel with intensive training and expertise in cyber defense and the infrastructure necessary to maintain a pool of specialists in cyber warfare. Education, research, manpower and operations for a proactive self-defense in cyberspace must be fully funded now to prevent a disaster in the future."--P. v.

Call No. U 163 .C946 2008

Janczewski, Lech and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: Information Science Reference, 2008.

Focus: "This book reviews problems, issues, and presentations of the newest research in the field of cyberwarfare and cyberterrorism. While enormous efficiencies have been gained as a result of computers and telecommunications technologies, use of these systems and networks translates into a major concentration of information resources, creating a vulnerability to a host of attacks and exploitations"--Provided by publisher.

Call No. U 163 .P853 2001

Price, Alfred. *War in the Fourth Dimension : US Electronic Warfare, from the Vietnam War to the Present*. Mechanisburg, PA: Stackpole, 2001.

Focus: "Electronic warfare aircraft; United States- Electronics in military engineering; United States- Military art and science; United States – Automation- Information warfare."

Call No. U 163 .T46 2005

Thomas, Timothy L. *Cyber Silhouettes: Shadows Over Information Operations*. Fort Leavenworth, KS: Foreign Military Studies Office (FMSO), 2005.

Focus: "Understanding our cyber environment; Engaging cyber or information ubiquity; Al Qaeda and the Internet: the danger of "cyberplanning"; Cyberinsurgency; Is the IW paradigm outdated? A discussion of US IW theory; Comparing US, Russian, and Chinese information operations concepts; Chinese and American network warfare; Applications and case studies in peace and war; Virtual peacemaking: a military view of conflict prevention through the use of information technology; Kosovo and the current myth of information superiority;

"Policekeeping" and the need for information technologies; Information warfare in the second (1999-present) Russian-Chechen war."

Call No. UA 23 .C929 2009

Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz. *Cyberpower and National Security*. Washington, D.C.: National Defense University, Center for Technology and National Security Policy, 2009.

Focus: "National security; Information technology-Government policy; Cyberspace-Government policy; Cyberterrorism."

Call No. UB 276 .P39 2008

Paul, Christopher. *Information Operations : Doctrine and Practice : A Reference Handbook*. Westport, CT: Praeger Security International, 2008.

Focus: "Psychological warfare; Information warfare."

Call No. Periodicals

Joint Information Operations Center (U.S.). *IO Sphere : The Professional Journal of Joint Information Operations*. San Antonio, TX: Joint Information Operations Center, 2005-

Focus: "Information warfare"

Alt. Title: Information operations sphere

Status: Currently Received

Call No. Internet Resource (click on the link in JFSC Library Catalog)

Taylor, Donald P. "Islamic extremists love the Internet." Master's Thesis, Joint Forces Staff College, Joint Advanced Warfighting School, 2009.

Focus: Thesis (M.S. in Joint Campaign Planning and Strategy)-- "Al-Qaeda and its network of followers have had great success during this decade with their efforts to influence the West. Which cyber tool have these terrorists used as their main weapon to achieve their objectives? What effect is this having on America's younger generation? Since September 11, 2001 Islamic extremist terrorists have been exploiting the Internet to promote their radical ideology and today they are targeting select youth, developing them into home-grown terrorists who support their cause. A careful study of select terror Web sites reflects that jihadists are promoting their propaganda and highlighting successful operations directed against our government and the US military. What cyber techniques are being used for persuasion? How are our leaders handling this threat? Is there more they can be doing? This author's thesis is that Islamic extremists are exploiting the Internet resulting in the development of homegrown terrorists a serious vulnerability which the US government has inadequately addressed."--Abstract

AUDIO/VISUAL MATERIALS

Call No. DVD C9

Kirk, Michael. *Cyber war!* DVD (Boston: Frontline WGBH Boston, PBS Home Video [distributor], 2003).

Focus: "Frontline investigates just how real the threat of war in cyberspace is and reveals what the White House knows that the rest of us don't."

SEARCHING JFSC LIBRARY RESOURCES

ProQuest

(subscription database; access via Blackboard)

Awan, A., and M. Al-Lami. "Al-Qa'ida's Virtual Crisis." *RUSI Journal* 56 (February 1, 2009).

Abstract: "The fight Al-Qa'ida has waged against the West has been fought on a virtual as well as physical battlefield. Recently, many jihadist strongholds and hiding places on the web have been shut down. This article charts the growth and the current crisis of Al-Qa'ida's 'media jihad'."

Seib, P. "The Al-Qaeda Media Machine." *Military Review* (May 1, 2008): 74-80.

Abstract: "Terrorism experts speculated that an Al-Qaeda condition for its affiliating with the North African Salafiti Group for Call and Combat was an upgrade of the local group's media competency. Even cartoons depicting children as suicide bombers are easily available on the Web, and Hamas's Al-Aqsa Television has featured children's programming that extols martyrdom. Recognizing the pervasiveness of the information delivered by satellite television and the Internet and the influence of news organizations ranging from the BBC to Al-Jazeera, Al-Qaeda is now offering, in the words of Michael Scheuer, "a reliable source of near real-time news coverage from the jihad fronts for Muslims.""

EBSCOhost

(subscription database; access via Blackboard)

Arwood, Sam, Robert Mills, and Richard Raines. "Operational art and Strategy in Cyberspace." *Proceedings of the International Conference on Information Warfare & Security* (January 2010): 16-22.

Abstract: "While there has been much written about cyberspace and the potential of cyber warfare in general, there is little discussion about specific cyber warfare theory—that is how cyberspace capabilities can be integrated with other traditional military capabilities to influence an adversary, achieve effects, and win wars. The purpose of this paper is to stimulate conversation about operational art in cyberspace. Specifically, we present a planning approach that ties together national strategy, instruments of national power, and a well-known targeting strategy for complex systems. The result is a method of selecting targets that can be traced to higher-level strategies and outcomes."

Gallerywatch

(CRS) (subscription database; access via Blackboard)

Figliola, Patricia M. *The Federal Networking and Information Technology Research and Development Program: Funding Issues and Activities*. Washington, DC: Congressional Research Service, 2010.

Abstract: "On November 18th, the House Committee on Science and Technology passed H.R. 4061, the Cybersecurity Enhancement Act of 2009, to improve the security of cyberspace by ensuring federal investments in cybersecurity are better focused, more effective, and that research into innovative, transformative technologies is supported. The bill addresses recommendations from the Administration's Cyberspace Policy Review and includes input from four hearings held on cybersecurity during the first session. H.R. 4061 would reauthorize and expand the Cyber Security Research and Development Act (P.L. 107-305). In addition to promoting cybersecurity R&D by the member agencies of the NITRD, the legislation addresses cybersecurity workforce concerns and advances the development of technical standards. H.R. 4061 is a combination of two Committee discussion drafts: the Cybersecurity Research and Development Amendments Act of 2009 and the

Cybersecurity Coordination and Awareness Act of 2009. The full House is expected to take action on this legislation in the near future. Bills: H.R. 4061 Document No.: RL33586”

PolicyFile

(subscription database; access via Blackboard)

Gregory C. Wilshusen, Director, Information Security Issues, testimony on Information Security: Concerted Response Needed to Resolve Persistent Weaknesses, on March 24, 2010, to the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives, *Government Accountability Office*, 2010.

URL: <http://www.gao.gov/new.items/d10536t.pdf>

Abstract: “Concerned by reports of weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. GAO was asked to testify on federal information security and agency efforts to comply with FISMA. This testimony summarizes (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. To prepare for this testimony, GAO analyzed its prior reports and those from 24 major federal agencies, their inspectors general, and the Office of Management and Budget (OMB).”

Lewis, James A. *Computer Espionage, Titan Rain and China*. Washington, DC: Center for Strategic and International Studies, 2005.

URL: http://csis.org/files/media/csis/pubs/051214_china_titan_rain.pdf

Abstract: “In 1998, computer networks in the Pentagon came under sustained ‘attack’ for several days. Solemn officials came to the conclusion that China was the attacker and they began to contemplate having the Department of Defense launching some kind of cyber counterstrike when a little more investigation showed that the attacker was not the Peoples Liberation Army but bored teenagers in Cupertino, California. Cyberwar averted, and a useful lesson to contemplate as we regard the latest round of computer network penetrations at DOD facilities attributed to the Chinese (named “Titan Rain”).”

Jane's Online

(subscription database; access via Blackboard)

Skinner, Tony. “War and PC: Cyberwarfare.” *Jane's Defence Weekly* (19 Sep 2008).

Abstract: “The cyber attacks that hit Georgian government websites as Russian tanks rolled into South Ossetia in August may have heralded the coming of age of a new dimension of warfare. As the conflict between the two countries escalated on the ground, Georgian websites were hit by concerted distributed denial of service (DDOS) cyber attacks. In one of the first examples of a military campaign being supported by a series of cyber attacks on opposition websites - albeit indirectly - the official website of Mikheil Saakashvili, the Georgian President, the central government site, as well as the home pages for the Ministry of Foreign Affairs and Ministry of Defence, were all affected in the days leading up to the conflict.”

“Total Gridlock - Cyber Threat to Critical Infrastructure.” *Jane's Intelligence Review* (12 Oct 2009).

Abstract: “Key Points -Critical infrastructure is dependent on technological control systems. The nature of their technological structure means that they could be vulnerable to cyber attacks, potentially damaging the functions of critical infrastructure. However, any such attack is more likely to be perpetrated by an insider than an external criminal or terrorist. Utility companies are particularly vulnerable to malicious internet-based

attacks. Levi Gundert examines how hackers could exploit flaws in technological control systems to cause widespread disruption to national electricity infrastructure.”

Praeger International

(subscription database; access via Blackboard)

Lailari, Guermantes E. “The Information Operations War Between Israel and Hizballah During the Summer of 2006.” In *Influence Warfare*, edited by James J. F. Forest. Westport, CT: Praeger Publishers, 2009.

Abstract: “The U.S. Government is becoming more interested in information operations (IO) especially as a result of its involvement in the Middle East. As a reflection of this, the Department of Defense (DoD) and the military services have developed a range of IO doctrines. Nonstate actors, on the other hand, such as terrorist groups, have been using IO adeptly for decades based on the necessity to strengthen their support base and counter their enemies' military advantages. In essence, IO is very useful for a terrorist group since it is often a cheap and powerful asymmetric tool against states, especially against regional or superpowers.”

Arquilla, John. “Information Wars.” In *Globalization and Security*, edited by G. Honor Fagan. Westport, CT: Praeger Publishers, 2009.

Abstract: “All the major technological advances of the Industrial Revolution, which began some two centuries ago, while initially aimed at improving commerce and society, quickly found their way into battle. Starting with the decades immediately after Waterloo (1815), steam engines came to power mass production and the ships and railroads that moved about large numbers of people and goods at hitherto unimagined sustained speeds. Soon thereafter, the electric telegraph completely replaced its optical predecessor, and vast amounts of information flowed by Morse code wherever the wires were set in place. These developments all had tremendous effects on commercial and social development. They also revolutionized warfare.”

The White House. “National Strategy to Secure Cyberspace, Executive Summary.” In *Homeland Security: Protecting America's Targets*. Westport, CT: Praeger Publishers, 2006.

Abstract: “Our Nation’s critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.”

Global Issues in Context

(subscription database; access via Blackboard)

Raghavan, R. "Cybercrime: Problems and Prospects." In *World Encyclopedia of Police Forces and Correctional Systems*, edited by George Kurian, 30-36. Detroit: Gale, 2006.

Homeland Security Digital Library

<https://hsdl.org>

Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment. Arlington, VA: Intelligence and National Security Alliance (INSA), 2009.

URL: http://www.insonline.org/assets/files/INSA_CyberAssurance_Assessment.pdf

Abstract: “the President commissioned a comprehensive cyber assurance study in order to identify public and private sectors that have a stake in cyber assurance, pose key questions to frame the relevant issues, articulate concerns, and formulate initial policies for our nation in this critical area. The Intelligence and National Security Alliance (INSA), which represents the defense, intelligence, national security, and telecommunications industries, formed a task force to address several of these questions. INSA worked with members of the defense, intelligence, national security, and telecommunications communities to address these questions.” Lewis, James A. *'Korean' Cyber Attacks and their Implications for Cyber Conflict*. Washington, D.C.: Center for Strategic and International Studies, 2009.

URL:

http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf

Abstract: "Topics discussed in this paper include: "When does a cyber attack become an act of war; Deterrence in cyberspace; Norms and thresholds; Political constraints on cyber attack; and Non-state actors in cyberspace." Points made by the author include: "Uncertainty in attribution, collateral damage, and effect, is the key feature of cyber conflict; Cyber conflict is shaped by implicit norms and thresholds; Militaries now have the capability to launch damaging cyber attacks against critical infrastructure, but serious cyber attack independent of a larger military conflict is unlikely; Non-state actors do not yet have the capability to launch a serious cyber attack, they will be able to acquire these from the cybercrime black market in less than a decade; The United States has pre-eminent offensive cyber capabilities, but it obtains little deterrent benefit from this; [and]The United States is uniquely vulnerable and would gain more from international engagement."

Ng, Chee Mun. *CyberCIEGE Scenario to Illustrate Classified Information Management in Multilevel Secure Systems for Military Command and Control*. Monterrey, CA: Naval Postgraduate School, 2005.

URL: https://www.hsdl.org/homesec/docs/theses/05Dec_Ng.pdf&code=ebc33a4b787c0ab31949d899bdab198f

Abstract: "Raising the awareness of information security has been the focus of DOD and other government agencies in recent years. There is a need for an effective means of educating and training personnel in the topic of Information Assurance. CyberCIEGE offers an approach to training by engaging the personnel in an interactive simulation-based network security game. Each game scenario in CyberCIEGE is designed to impart some network security principles and Information Assurance concepts to the players."

Phister, Paul W., Daniel Fayette and Emily Krzysiac. *CyberCraft: Concept Linking NCW Principals with the Cyber Domain in an Urban Operational Environment*. Wright-Patterson Air Force Base, OH: Air Force Research Laboratory, Information Directorate, 2005.

URL: <https://www.hsdl.org/homesec/docs/dtic/ADA464201.pdf&code=ebc33a4b787c0ab31949d899bdab198f>

Abstract: "With the entry into the Information Age comes a new theory of warfare; Network Centric Warfare (NCW). Currently, discussions regarding NCW have concentrated on the traditional forms of warfare, namely those that occur within the sub-surface, surface, air and space mediums. Additionally, limited discussions have centered on the asymmetric aspect of the new threat, i.e., joint urban operations. Great strides are being made linking NCW to asymmetric threats, but again these have centered on sub-surface, surface, air and space mediums. There is another medium that can be utilized that has the potential of becoming the most effective use of military force in the Information Age. Using the Cyber Domain to conduct military operations within an urban environment has significant potential. This paper presents an introduction of a new 'cyber vehicle', called the 'CyberCraft', which performs similar operations as conventional vehicles, such as a strike platform (e.g., deny, destroy, degrade, disrupt or deceive) or as an 'Intelligence Surveillance Reconnaissance (ISR)' platform (e.g., find, fix, track, monitor); however, the 'CyberCraft' operates solely within the cyber domain to extend the arm of military application of force."

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

URL: <https://hsdl.org/?view&doc=108265&coll=documents>

Abstract: “In January 2008, the Bush Administration established the Comprehensive National Cybersecurity Initiative (the CNCI) by a classified joint presidential directive. [...] In response to the CNCI and other proposals, questions have emerged regarding: (1) the adequacy of existing legal authorities—statutory or constitutional—for responding to cyber threats; and (2) the appropriate roles for the executive and legislative branches in addressing cybersecurity.” Report Number: CRS Report for Congress, R40427

Defense.gov

<http://www.defense.gov>

Garamone, Jim. “Obama Announces Cyber Security Office.” *American Forces Press Service* (May 29, 2009).

Abstract: “The nation’s computer network infrastructure will be defended as a national strategic asset, President Barack Obama said here today.”

Lynn, William J. “Speech on Cyber Security at the Center for Strategic and International Studies as Delivered by Deputy Secretary of Defense, William J. Lynn.” Center for Strategic and International Studies, Washington, D.C., June 15, 2009.

URL: <http://www.defense.gov/speeches/speech.aspx?speechid=1365>

Abstract: “As the president said at the Naval Academy, quote, “We must overcome the full spectrum of threats. This includes the nation-state and the terrorist network, the spread of deadly technologies and the spread of hateful ideologies, 18th century piracy and 21st century cyberthreats.””

CIAO

(subscription database; access via Blackboard)

Powell, Benjamin. *Is Cybersecurity a Public Good? Evidence from the Financial Services Industry*. San Jose, CA: Independent Institute, 2005.

Abstract: “The September 11, 2001, terrorist attacks on the United States heightened concerns about vulnerabilities to future attacks. One new area of concern is cyberterrorism: the possibility of terrorists using computers to attack our critical infrastructure electronically. The government has made efforts to better secure its own computer networks to prevent terrorists from hacking into computer systems in the Pentagon, FBI, and other government agencies. Increasingly, however, the government has been concerned that the private sector is vulnerable to cyberterrorism. The private sector owns approximately 85 percent of the critical infrastructure in the U.S. (Deloitte 2004 p. 15). There are concerns that a cyber attack on dams, trains, electrical grids, pipeline pumps, communications networks, or the financial services industry could cause significant physical or economic damage to the U.S. The policy question being asked is whether private businesses, when left to their own devices, provide enough cybersecurity or if some form of government involvement is justified.”

CQ Researcher

(subscription database; access via Blackboard)

Marshall, P. “Cybersecurity.” *CQ Researcher* 20 (February 26, 2010): 169-192.

Abstract: “The recent attacks on Google servers, apparently launched from China, underscore the threat cyberattacks pose to American individuals and businesses as well as to national security. In addition to billions of dollars being stolen by cybercriminals, military secrets and critical civilian infrastructure — including

utilities, transportation and finance — also are at risk. Indeed, attempted attacks on Pentagon computers alone number in the tens of thousands each year. The hackers range from international gangs to the agents of other countries. Lawmakers and cybersecurity analysts agree the U.S. is woefully unprepared to deal with the challenge. Civilian and military leaders say they are ramping up defensive efforts, but many experts warn that the measures proposed are inadequate. Some analysts argue that to counter the threat the United States will not only have to spend hundreds of billions of dollars but also fundamentally change the way Americans work with computers and the Internet.”

Defense Technical Information Center

<http://www.dtic.mil/>

Ashmore, William C. *Impact of Alleged Russian Cyber Attacks*. Monograph. Fort Leavenworth, KS: Army Command and General Staff College, May 2009.

URL: <http://handle.dtic.mil/100.2/ADA504991>

Abstract: “The cyber attacks that have occurred in the last few years have shown the vulnerabilities of using the internet and the weaknesses of cyber defenses. Regional organizations, such as the North Atlantic Treaty Organization (NATO) and the European Union (EU), and international organizations, such as the United Nations (UN), have been inadequate in preventing cyber attacks for political purposes and bringing cyber criminals to justice. Government and organizational leaders need to ensure that their cyber defenses are ready to protect private information, internet services, and electrical grids that rely on internet technology to function. Former Soviet satellites, the United States, and international organizations need to increase their cooperation to defeat cyber crime. Without a legal international opposition, cyber criminals will continue to operate in areas where there are no laws or agreements concerning cyber security. Nations can build their own defenses, but cooperation and the sharing of technical data will enable a safer internet environment for everyone.”

Boyd, Bradley L. “Cyber Warfare: Armageddon in a Teacup?” Master's thesis, Army Command and General Staff College, 2009.

URL: <http://handle.dtic.mil/100.2/ADA512381>

Abstract: “Security concerns over the growing capability of Cyber Warfare are in the forefront of national policy and security discussions. In order to enable a realistic discussion of the topic this thesis seeks to analyze demonstrated Cyber Warfare capability and its ability to achieve strategic political objectives. This study examines Cyber Warfare conducted against Estonia in 2007, Georgia in 2008, and Israel in 2008. In all three cases Cyber Warfare did not achieve strategic political objectives on its own. Cyber Warfare employed in the three cases consisted mainly of Denial of Service attacks and website defacement. These attacks were a significant inconvenience to the affected nations, but the attacks were not of sufficient scope, sophistication, or duration to force a concession from the targeted nation. Cyber Warfare offensive capability does not outmatch defensive capability to the extent that would allow the achievement of a strategic political objective through Cyber Warfare alone. The possibility of strategic level Cyber Warfare remains great, but the capability has not been demonstrated at this time.”

Connary, Shane M. *Computer Network Operations Command and Control: A New Perspective*. Final rept. Newport, RI: Naval War College, October 22, 2009.

URL: <http://handle.dtic.mil/100.2/ADA513948>

Abstract: “Our national security is inextricably linked to the cyberspace domain, where conflict is not limited by geography or time. The standup of United States Cyber Command in September 2009 was a milestone in cyberspace command and control (C2). However, the DOD continues to struggle in developing the proper doctrine, organizations, and processes to execute the cyberspace mission across the range of military operations.

Using a cyber scenario as a backdrop, this paper examines some of the complex challenges operational commanders face concerning cyberspace C2. It discusses current doctrine disconnects, Computer Network Operations fundamentals, the information environment and cyberspace's role in it, as well as the levels of warfare. Finally, the paper contrasts two possible models for cyberspace C2 at the operational level of command, and provides recommendations to meet the cyberspace challenges.”

Dobitz, Kyle, Brad Haas, Michael Holtje, Amanda Jokerst, Geoff Ochsner, Stephanie Silva, Kevin Johnson, and John G Hudson II. *The Characterization and Measurement of Cyber Warfare*. Omaha, NE: Global Innovation and Strategy Center , 2008.

URL: <http://handle.dtic.mil/100.2/ADA497907>

Abstract: “Hostile exercises across computer networks are today increasingly common, and the proliferation of such activity is a national security concern. The characterization of cyberspace activity is the subject of much debate; the unique nature of the cyber arena calls into question traditional state boundaries and operational codes of conduct. Actors in cyberspace can exhibit influence from anywhere in the world, thus many hostile acts are difficult to trace. Additionally, targets in cyberspace are often intangible, rendering an appropriate response that is difficult to discern. This report provides a framework useful for delineating such acts, utilizing existing literature and current international law as a frame. Additionally, this research utilized the assumption that all actors and actions in cyberspace carry inherent risks, and did not separate bad actions from good. The following factors were identified by the research team as critical for purposes of cyber act characterization: Motivation, Intent, Target, Effects, and Actors.”

Greene, Christopher V. *Cyberwarfare and Our Allies: The Importance of Theater Security Cooperation*. Final rept. Newport, RI: Naval War College, October 23, 2009.

URL: <http://handle.dtic.mil/100.2/ADA513954>

Abstract: “Russia's future use, either state sponsored or through proxies, of cyber attacks to influence NATO Allied domestic decisions regarding energy, missile defense, and security should be expected. The Commander, U.S. EUCOM, is faced with a complex issue, which has the potential to threaten all instruments of national power. This paper will apply the elements of operational art, specifically operational factors and functions, to illustrate why EUCOM must integrate combating cyberwarfare in its theater security cooperation efforts to better prepare NATO Allies for a cyber attack. It delves into the complexity of the cyberwarfare security issue and identifies the need to mitigate vulnerabilities before they can be exploited, advocating the need for enhanced security cooperation efforts. Finally, the paper provides a recommended security cooperation framework to establish priority and unity of effort across the many disparate organizations involved in addressing this complex security issue.”

Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Mclean, VA: Northrop Grumman Corp, 2009.

URL: <http://handle.dtic.mil/100.2/ADA509000>

Abstract: “This paper presents a comprehensive open source assessment of China's capability to conduct computer network operations (CNO) both during peacetime and periods of conflict. The result will hopefully serve as useful reference to policymakers, China specialists, and information operations professionals. The research for this project encompassed five broad categories to show how the People's Republic of China (PRC) is pursuing computer network operations (CNO) and the extent to which it is being implemented by examining: a) The PLA's strategy for computer network operations at the campaign and strategic level to understand how China is integrating this capability into overall planning efforts and operationalizing it among its field units; b) Who are the principal institutional and individual actors in Chinese CNO and what linkages may exist between the civilian and military operators;

- c) Possible targets of Chinese CNO against the US during a conflict to understand how the PLA might attempt to seize information control over the US or similar technologically advanced military during a conflict;
- d) The characteristics of ongoing network exploitation activities targeting the US Government and private sector that are frequently attributed to China;
- e) A timeline of alleged Chinese intrusions into US government and industry networks to provide broader context for these activities.”

Miller, Robert A., and Daniel T. Kuehl. “Cyberspace and the “First Battle” in 21st-century War.” *Defense Horizons* 68 (Sep 2009).

URL: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA508696&Location=U2&doc=GetTRDoc.pdf>

Abstract: “Coordinated cyber attacks designed to shape the larger battlespace and influence a wide range of forces and levers of power may become the key feature of the next war. Early forms of this may have already been seen in Estonia and Georgia. Control of cyberspace may thus be as decisive in the network dependent early 21st century as control of the air was for most of the 20th century. In the future, cyber attacks may be combined with other means to inflict paralyzing damage to a nation’s critical infrastructure as well as psychological operations designed to create fear, uncertainty, and doubt, a concept we refer to as infrastructure and information operations. The cyber sphere itself is, of course, a critical warfighting domain that hosts countless information infrastructures, but the rise of network based control systems in areas as diverse as the power grid and logistics has widened the threat posed by network attacks on opposing infrastructures.”

Rauch, Daniel E. *Electronic Warfare for Cyber Warriors*. Graduate Research Project. Patterson Air Force Base, OH: Air Force Inst of Tech Wright, School of Engineering and Management, June 2008.

URL: <http://handle.dtic.mil/100.2/ADA487250>

Abstract: “This research paper provides complete course content for the AFIT EENG 509, Electronic Warfare class. It is intended as a replacement for the existing course and designed for Intermediate Developmental Education (IDE) students in the Cyber Warfare degree program. This course provides relevant academic courseware and study material to give cyber warriors an academic and operational perspective on electronic warfare and its integration in the cyber domain.”

Google & Government Google

<http://www.google.com/unclesam>

*You can use the Advanced search to limit your results to .edu, .mil, .gov & .org websites.

Chen, Hsinchun, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, and Gabriel Weimann. *Uncovering the DarkWeb: A Case Study of Jihad on the Web*. Silver Spring, MD: ASIS&T, 2008.

Abstract: “While the Web has become a worldwide platform for communication, terrorists share their ideology and communicate with members on the “DarkWeb”—the reverse side of the Web used by terrorists. Currently, the problems of information overload and difficulty to obtain a comprehensive picture of terrorist activities hinder effective and efficient analysis of terrorist information on the Web. To improve understanding of terrorist activities, we have developed a novel methodology for collecting and analyzing Dark Web information. The methodology incorporates information collection, analysis, and visualization techniques, and exploits various Web information sources. We applied it to collecting and analyzing information of 39 Jihad Web sites and developed visualization of their site contents, relationships, and activity levels. An expert evaluation showed that the methodology is very useful and promising, having a high potential to assist in investigation and understanding of terrorist activities by producing results that could potentially help guide both policymaking and intelligence research.” © 2008 ASIS&T • Published online 7 April 2008 in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/asi.20838

CHIPS. U.S. Navy IT Umbrella Program and the Department of the Navy Chief Information Officer. 1982-

URL: http://www.chips.navy.mil/archives/10_apr/web_pages/index.html

Abstract: “Every issue is packed with cutting-edge technology topics, such as FORCEnet; knowledge dominance; C4ISR and network-centric warfare programs; e-business; e-learning; professional development — and interviews with top leadership from the DON and DoD.”

Critical Issues for Cyber Assurance Policy Reform: An Industry Assessment

Publisher: Intelligence and National Security Alliance (INSA)

Date: 2009-01-01

Copyright: 2009 Intelligence and National Security Alliance.

URL: http://www.insonline.org/assets/files/INSA_CyberAssurance_Assessment.pdf

Crosstalk: The Journal of Defense Software Engineering. Ogden Air Logistics Center, Hill AFB: Software Technology Support Center, 1994-

URL: <http://www.stsc.hill.af.mil/crosstalk/2010/05/index.html>

Abstract: “CrossTalk’s mission is to encourage the engineering development of software in order to improve the reliability, sustainability, and responsiveness of our warfighting capability and to inform and educate readers on up-to-date policy decisions and new software engineering technologies.”

Gasper, Peter D. “Cyber Threat to Critical Infrastructure 2010-2015.” Presented at the Information & Cyberspace Symposium, Fort Leavenworth, Kansas, September 22-24, 2008.

URL: http://usacac.army.mil/cac2/cew/nexus/NEXUS_VOL_2-1_-_Peter_Gasper.pdf

Abstract: “Trends in Critical Infrastructure (CI) Control Systems (CS): Although a dramatic technological leap forward in CS in the CI environment is not forecast for the period 2010-2015, trends in key CS technologies must be noted. Viewed together, these trends indicate the future operational environment will be populated with more CS in the CI sector, and those systems will have more communications elements. Thus, the CS impact on the future operational environment will be increased presence and exposure to threat sources. Trend 1 – Proliferation of Control Systems... Trend 2 – Increased Digital and IP Base... Trend 3 – Expanded Use of Wireless Communications”

Georgia Tech Information Security Center (GTISC). *Emerging Cyber Threats Report for 2009 Data, Mobility and Questions of Responsibility will Drive Cyber Threats in 2009 and Beyond on October 15, 2008*. Atlanta, GA: Georgia Tech Information Security Center, 2008.

URL: <http://www.gtisc.gatech.edu/>

Abstract: “The Georgia Tech Information Security Center (GTISC) hosted its annual summit on emerging security threats and countermeasures affecting the digital world. At the conclusion of the event, GTISC released this Emerging Cyber Threats Report—outlining the top five information security threats and challenges facing both consumer and business users in 2009. This year’s summit participants include security experts from the public sector, private enterprise and academia, reinforcing GTISC’s collaborative approach to addressing information security technology and policy challenges.”

Kruzell, John J. "Cyber Warfare a Major Challenge, DoD Official Says." *Air Force Print News Today* (March 6, 2008).

URL: http://www.fairchild.af.mil/news/story_print.asp?id=123089250

Abstract: "Deputy Defense Secretary Gordon England is the latest government official to express concern about the United States' cyberspace vulnerabilities."

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Arlington, VA: RAND, 2009.

URL: <http://www.rand.org/pubs/monographs/MG877/>

Abstract: "The protection of cyberspace, the information medium, has become a vital national interest because of its importance both to the economy and to military power. An attacker may tamper with networks to steal information for the money or to disrupt operations. Future wars are likely to be carried out, in part or perhaps entirely, in cyberspace. It might therefore seem obvious that maneuvering in cyberspace is like maneuvering in other media, but nothing would be more misleading. Cyberspace has its own laws; for instance, it is easy to hide identities and difficult to predict or even understand battle damage, and attacks deplete themselves quickly. Cyberwar is nothing so much as the manipulation of ambiguity. The author explores these topics in detail and uses the results to address such issues as the pros and cons of counterattack, the value of deterrence and vigilance, and other actions the United States and the U.S. Air Force can take to protect itself in the face of deliberate cyberattack."

Rid, Thomas. *War 2.0*. Stanford, CA: Leland Stanford Junior University, 2007.

URL: <http://www.hoover.org/publications/policyreview/5956806.html>

Abstract: "Marked most visibly by the technologically sophisticated first war against Iraq in 1991, the U.S. Defense Department's project of military transformation was widely celebrated as a "revolution in military affairs" of historical dimensions. Never before had an army acquired such awe-inspiring technological superiority over virtually all possible adversaries. Officers all around the world adapted the basic concept of transformation, or "network-centric operations" in the military's idiom. But the movement threatened to turn into an inward-looking technology exercise, with a narrow focus on high-tech projects such as blue-force-tracker, an astronomically expensive system to monitor the actual position of all American forces in real-time, or high-resolution overhead imagery and even live video-feeds, beamed into command headquarters by satellites and drones. Real-time signal intelligence from the sky was to be instantly connected with massive firepower on the ground to enhance the 21st-century warfighting machine's efficiency and lethality."

Schwartz, Norty. "Space, Cyberspace, and National Security." Prepared Speech for Delivery, Orlando, FL, Air Force Association, February 18, 2010.

URL: <http://www.af.mil/shared/media/document/AFD-100219-034.pdf>

Abstract: "Today, I would like to discuss matters involving the ultimate high ground of space, and the still largely undiscovered possibilities in the emerging medium of cyberspace. Virtually all aspects of military operations are affected in some way by the capabilities provided from these domains, and it's difficult to overstate their importance to the success of our armed forces. From precision navigation and timing, to global satellite communications, to space-based surveillance and missile warning, our space assets provide us with an unparalleled degree of accuracy, connectivity, and situational awareness. And, our exploitation of cyberspace and advanced information technologies enable us and the Joint team to properly command and control our forces, binding virtually all of our advanced capabilities together into precise, increasingly networked, and better synchronized operations."

U. S. MILITARY & GOVERNMENT LINKS

Internet Links

Air Force Institute of Technology. "Center for Cyberspace Research."

<http://www.afit.edu/en/ccr/index.cfm>

Focus: "The Center for Cyberspace Research, established in March 2002, conducts defense-focused research at the Master's and PhD levels. The CCR is forward-looking and responsive to the changing educational and research needs of the Air Force, Department of Defense, and the federal government. The CCR faculty teaches and performs research focusing on understanding and developing advanced cyber-related theories and technologies. These theory and technology advancements have included efforts in network intrusion detection and avoidance, insider threat mitigation, cyberspace situational awareness, network visualization, software protection, and anti-tamper technologies development."

Analytic Services Inc. "HSI Home Page." Homeland Security Institute.

<http://www.homelandsecurity.org>

Friedman, George. "Cyberwarfare." STRATFOR.

<http://www.stratfor.com/theme/cyberwarfare>

Focus: "STRATFOR delivers critical intelligence and perspective through: Situation Reports: Snapshots of global breaking news; Analysis: Daily reports that assess key world events and their significance; Quarterly & Annual Forecasts: Rigorous predictions of what will happen next; Multimedia: Engaging videos and information-rich interactive maps; Intelligence Guidance: Internal memos that guide STRATFOR staff in their intelligence-gathering operations in the immediate days ahead."

National Defense University. "Challenges in International Cyber Security." Center for Technology and National Security Policy.

<http://www.ndu.edu/CTNSP/index.cfm>

Focus: "The Center for Technology and National Security Policy (CTNSP) examines the implications of technological innovation for U.S. national security policy and military planning. CTNSP combines scientific and technical assessments with analyses of current strategic and defense policy issues, taking on topics to bridge the gap. The Center has produced studies on proliferation and homeland security, military transformation, international science and technology, information technology, life sciences, and social science modeling."

National Security Council. "Cybersecurity." Executive Office of the President.

<http://www.whitehouse.gov/administration/eop/nsc/cybersecurity>

Focus: "As a result, the President directed a top-to-bottom review of the Federal Government's efforts to defend our information and communications infrastructure, which resulted in a report titled the Cyberspace Policy Review. To implement the results of this review, the President has appointed Howard Schmidt to serve at the U.S. Cybersecurity Coordinator and created the Cybersecurity Office within the National Security Staff, which works closely with the Federal Chief Information Officer Vivek Kundra, the Federal Chief Technology Officer, Officer Aneesh Chopra and the National Economic Council."

National Science Foundation. "Directorate for Computer and Information Science and Engineering."

<http://www.nsf.gov/dir/index.jsp?org=CISE>

Focus: "The Directorate for Computer and Information Science and Engineering has three goals: to enable the U.S. to uphold a position of world leadership in computing, communications, and information science and

engineering; to promote understanding of the principles and uses of advanced computing, communications and information systems in service to society; to contribute to universal, transparent and affordable participation in an information-based society. To achieve these, CISE supports investigator initiated research in all areas of computer and information science and engineering, helps develop and maintain cutting-edge national computing and information infrastructure for research and education generally, and contributes to the education and training of the next generation of computer scientists and engineers.”

Space and Naval Warfare Systems Command (SPAWAR). “Program Executive Office C4I.”

<http://enterprise.spawar.navy.mil/>

Focus: “The mission of PEO C4I is to provide integrated communications and information technology systems, and the end-to-end connectivity needed to enable decision superiority and ensure the mission success of our naval forces. PEO C4I acquires, fields, and supports C4I systems that extend across Navy, joint, and coalition platforms. This includes managing acquisition programs and projects that cover all C4I disciplines: applications, networks, communications, intelligence and surveillance, and reconnaissance systems for afloat platforms and shore commands.”

U.S. Department of Defense. “Joint Task Force - Global Network Operations.”

<https://www.jtfgno.mil/misc/mission.htm>

Focus: “The JTF-GNO directs the operation and defense of the Global Information Grid across strategic, operational, and tactical boundaries in support of DoD’s full spectrum of war fighting, intelligence, and business operations.”

U.S. Department of Homeland Security. “National Cyber Security Division.”

http://www.dhs.gov/xabout/structure/editorial_0839.shtm

Focus: “Mission: The National Cyber Security Division (NCSD) works collaboratively with public, private and international entities to secure cyberspace and America’s cyber assets.”

U.S. Department of Homeland Security. “United States Computer Emergency Readiness Team (US-CERT).”

<http://www.us-cert.gov/>

Focus: “US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. Information is available from the US-CERT web site, mailing lists, and RSS channels.”

United States Naval Academy. "Cyber Warfare Activity - USNA Center for Cyber Security Studies."

<http://www.usna.edu/cyber/mids/cyberActivity.php>

Focus: “MISSION: Enhance the education of midshipmen in all areas of cyber security and operations; to facilitate the sharing of expertise and perspectives in cyber-enabled technologies from across the Yard; to provide a streamlined means of identifying priorities; to enhance inter-disciplinary research; and to disseminate information, harmonize efforts and shape a common framework for related cyber-enabled mission efforts at USNA.”

U.S. STRATCOM

<http://www.stratcom.mil>

U.S. GOVERNMENT & MILITARY DOCUMENTS, CONGRESSIONAL TESTIMONY & LEGISLATION

Joint Electronic Library

<http://www.dtic.mil/doctrine/>

U.S. Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Incorporating Change 1 - 20 March 2009). Joint Chiefs of Staff. Washington, DC: May 02 2007.

U.S. Joint Chiefs of Staff. *Joint Operations*, Joint Publication 3-0. Joint Chiefs of Staff. Washington, DC: February 13 2008.

U.S. Joint Chiefs of Staff. *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, Vol I*, Joint Publication 3-08. Joint Chiefs of Staff. Washington DC: March 17 2006.

U.S. Joint Chiefs of Staff. *Information Operations*, Joint Publication 3-13. Joint Chiefs of Staff. Washington, DC: February 13 2006.

U.S. Joint Chiefs of Staff. *Joint Operation Planning*, Joint Publication 5-0. Joint Chiefs of Staff. Washington, DC: December 26 2006.

DoD Issuances

<http://www.dtic.mil/whs/directives/corres/pub1.html>

U.S. Department of Defense. *DoD Directive 3020.40: DoD Policy and Responsibilities for Critical Infrastructure*, January 14, 2010.

URL: <http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf>

U.S. Department of Defense. *DoD Directive 5505.13E, DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)*, March 1, 2010.

URL: <http://www.dtic.mil/whs/directives/corres/pdf/550513E.pdf>

U.S. Department of Defense. *DoD Instruction 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, January 29, 2010.

URL: <http://www.dtic.mil/whs/directives/corres/pdf/520513p.pdf>

U.S. Department of Defense. *DoD Directive 3020.40, DoD Policy and Responsibilities for Critical Infrastructure*, January 14, 2010.

URL: <http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf>

U.S. Department of Defense. *DoD Instruction 5240.19, Counterintelligence Support to the Defense Critical Infrastructure, Counterintelligence Support to the Defense Critical Infrastructure Program*, August 27, 2007.

URL: <http://www.dtic.mil/whs/directives/corres/pdf/524019p.pdf>

U.S. Department of Defense. *DoD Instruction 1100.22, Policy and Procedures for Determining Workforce Mix*, April 12, 2010.

URL: <http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf>

DTIC

Blair, Dennis C. *Annual Threat Assessment of the US Intelligence Community for the House Permanent Select Committee on Intelligence*. Washington, D.C.: Office of the Director of National Intelligence, 2010.

URL: <http://handle.dtic.mil/100.2/ADA514115>

Abstract: “The recent intrusions reported by Google are a stark reminder of the importance of these cyber assets, and a wake-up call to those who have not taken this problem seriously. Companies who promptly report cyber intrusions to government authorities greatly help us to understand and address the range of cyber threats that face us all. I am here today to stress that, acting independently, neither the US Government nor the private sector can fully control or protect the country's information infrastructure. Yet, with increased national attention and investment in cyber security initiatives, I am confident the United States can implement measures to mitigate this negative situation.”

Theohary, Catherine A., and John Rollins. *Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress*. Washington, D.C.: Library of Congress Congressional Research Service, 2009.

URL: <http://handle.dtic.mil/100.2/ADA508928>

Abstract: “The proposed National Defense Authorization Act for Fiscal Year 2010 and the Intelligence Authorization Act for Fiscal Year 2010 both contain provisions that would affect programs and funding for current and future cybersecurity-related programs. In May 2009, the Obama Administration issued its 60-day review of cybersecurity policy, declaring that U.S. information networks would be treated as a strategic national asset. There is no single congressional committee or executive agency with primary responsibility over all aspects of cybersecurity; each entity involved pursues cybersecurity from a limited vantage point dictated by committee jurisdiction. Many different initiatives exist, but because of fragmentation of missions and responsibilities, stove-piping, and a lack of mutual awareness between stakeholders, it is difficult to ascertain where there may be programmatic overlap or gaps in cybersecurity policy. Drawing from common themes found in the Comprehensive National Cybersecurity Initiative (CNCI), a study by the Center for Strategic and International Studies (CSIS) Commission for the 44th Presidency, and the proposed near-term action plan from the President's recent Cyberspace Policy Review, this report identifies priority areas in cybersecurity for policy consideration. The report then lists and synthesizes current legislation that has been developed to address various aspects of the cybersecurity problem. It then lists the current status of the legislation and compares legislation with existing executive branch initiatives. Finally, analysis of information contained in executive branch initiatives and congressional legislation is used to offer cybersecurity-related considerations for Congress.”

CQ.com

(subscription database; access via Blackboard)

United States Government Accountability Office. *Cybersecurity Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*. Washington, D.C.: Government Accountability Office, 2010.

Abstract: “Pervasive and sustained cyber attacks against the United States continue to pose the threat of a potentially devastating impact on federal systems and operations. In January 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), establishing the Comprehensive National Cybersecurity Initiative (CNCI), a set of projects aimed at

safeguarding executive branch information systems by reducing potential vulnerabilities, protecting against intrusion attempts, and anticipating future threats. Shortly after taking office, President Obama, in February 2009, ordered a review of cybersecurity-related plans, programs, and activities underway throughout the federal government, including the CNCI projects. This review resulted in a May 2009 report that made recommendations for achieving a more reliable, resilient, and trustworthy digital infrastructure.”

Quadrennial Defense Review. Washington, D.C.: Government Printing Office, 2010.

Focus: Cyber Security issues are discussed throughout the document, special focus on page 37-39. Do an Edit-Find search for the term cyber to search the document.

Committee Passes Legislation to Improve Cybersecurity R&D (Press Release From the House Science and Technology Committee). Washington, D.C.: CQ Hot Docs, 2009.

Abstract: “Today, the House Committee on Science and Technology passed H.R. 4061 , the Cybersecurity Enhancement Act of 2009, by a voice vote. H.R. 4061 will improve the security of cyberspace by ensuring federal investments in cybersecurity are better focused, more effective, and that research into innovative, transformative technologies is supported. H.R. 4061 does this by reauthorizing and expanding the Cyber Security Research and Development Act (P.L. 107-305) passed by the Committee on Science and Technology in 2002. In addition to promoting cybersecurity R&D, the legislation addresses cybersecurity workforce concerns and advances the development of technical standards. H.R. 4061 is a combination of two Committee discussion drafts: the Cybersecurity Research and Development Amendments Act of 2009 and the Cybersecurity Coordination and Awareness Act of 2009.”

Anderson, Joanna. “House Bill Would Expand Research for Cyber-Attacks.” *CQ Weekly* (March 22, 2010): 701.

Abstract: “Cybersecurity and other homeland security research programs would be expanded under a bill approved by a House Homeland Security panel. The legislation (HR 4842), approved by the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology by voice vote March 16, would authorize roughly \$1 billion in each of fiscal years 2011 and 2012 for the Science and Technology Directorate, the department’s primary research and development arm. The bill would authorize \$150 million for cybersecurity research and development, with an emphasis on developing ways to deal with large-scale attacks. The subcommittee adopted by voice vote an amendment by Mary Jo Kilroy, D-Ohio, to include cyber forensics and attack-attribution research, which helps trace the source of a cyber-attack, under the program’s umbrella. The bill would also require the Homeland Security Department to probe whether the security of federally owned critical electric infrastructure has been compromised. Subcommittee Chairwoman Yvette D. Clarke, D-N.Y., said the bill was an acknowledgement of “the importance of science and technology research, development, testing and evaluation to ensuring the safety and security of the American people and our nation.”

United States Government Accountability Office. *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*. Washington, D.C.: Government Accountability Office, March 2010.

GAO-10-296

Abstract: “DHS issued the National Infrastructure Protection Plan (NIPP) in June 2006 to provide the approach for integrating the nation’s CIKR. GAO was asked to study DHS’s January 2009 revisions to the NIPP in light of a debate over whether DHS has emphasized protection—to deter threats, mitigate vulnerabilities, or minimize the consequences of disasters---rather than resilience---to resist, absorb, or successfully adapt, respond to, or recover from disasters. This report discusses (1) how the 2009 NIPP changed compared to the 2006 NIPP and (2) how DHS and SSAs addressed resiliency as part of their planning efforts. GAO compared

the 2006 and 2009 NIPPs, analyzed documents, including NIPP Implementation Guides and sector-specific plans, and interviewed DHS and SSA officials from all 18 sectors about their process to identify potential revisions to the NIPP and address resiliency.”

Government Accountability Office

<http://gao.gov>

Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment. Washington, D.C.: September 2009. GAO-09-969

Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities. Washington, D.C.: September 16, 2008. GAO-08-1157T

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. Washington, D.C.: September 9, 2008. GAO-08-825

Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks. Washington, D.C.: June 26, 2008. GAO-08-607

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. Washington, D.C.: July 31, 2008. GAO-08-588

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. Washington, D.C.: June 25, 2009. GAO-09-835T

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. Washington, D.C.: May 5, 2009. GAO-09-661T

Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks. Washington, D.C.: May 21, 2008. GAO-08-526

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. Washington, D.C.: March 10, 2009. GAO-09-432T

CYBER ISSUES WEBSITES

Council of Europe. “Convention on Cybercrime: Treaties.”

<http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?MA=49&CM=7&CL=ENG>

Focus: “The conventions of the Council of Europe are not statutory acts of the Organisation. They owe their legal existence to the consent of those member States that sign and ratify them. Furthermore, the great majority of the conventions of the Council of Europe make provision for non-member States of the Organisation to become Parties thereto, upon invitation by the Committee of the Ministers of the Council of Europe and by means of the procedure of accession.”

Cyber Conflict Studies Association (CCSA).

<http://www.cyberconflict.org/>

Focus: “CCSA is a 501(c)3 non-profit organization dedicated to promoting and leading a diversified research agenda in the field of cyber conflict. CCSA's vision is to be the premier thought leader in the field by fostering dialogue, leading research, and developing academic programs focused on the implications of cyber conflict. To achieve this, CCSA promotes and leads international intellectual development efforts to advance the field of cyber conflict research. These activities include workshops that bring together professionals from industry, academia and government to discuss strategic issues surrounding cyber conflict and the publication of insightful research articles and position papers in its Journal of Cyber Conflict Studies. CCSA also plays an important role in our national cyber-readiness strategy, serving as a resource for national security decision-makers and helping to frame and promote national cyber conflict policy.”

Georgia Institute of Technology. “Information Security Center.”

<http://www.gtisc.gatech.edu/>

Focus: “Invent and evaluate the key innovative user-centric security technologies and policies that will yield significant impact. Educate future researchers, policy makers, and information security leaders, and train current professionals in the most up-to-date methods for securing information systems. Provide a trusted set of resources and a safe haven where individuals and industrial, academic, and government organizations can access, understand, and evaluate issues related to new technologies and policies.”

National Academies Press – *Computers and Information Technology*

<http://www.nap.edu/topics.php?topic=279>

NATO. “Cooperative Cyber Defence Centre of Excellence.”

<http://www.ccdcoe.org/>

Focus: “The Cooperative Cyber Defence Centre of Excellence (CCD COE) was formally established on the 14th of May, 2008, in order to enhance NATO’s cyber defence capability. Located in Tallinn, Estonia, the Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic, and Spain as Sponsoring Nations.”

Open Net Initiative (ONI).

<http://opennet.net/research/profiles>

Focus: “Country profiles offer a synopsis of the findings and conclusions of our research into the factors influencing specific countries’ decisions to filter or abstain from filtering the Internet, as well as the impact, relevance, and efficacy of technical filtering in a broader context of Internet censorship. These profiles cover the countries where ONI conducted technical testing and analysis. Countries selected for in-depth analysis are those in which it is believed that there is the most to learn about the extent and processes of Internet filtering. Each country profile includes the summary results of the empirical testing for filtering.”

Purdue University. “Center for Education and Research in Information Assurance and Security (CERIAS).”

<http://www.cerias.purdue.edu/>

Focus: “Currently viewed as one of the world’s leading centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure. CERIAS is unique among such national centers in its multidisciplinary approach to the problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc) to ethical, legal, educational, communicational, linguistic, and economic issues, and the subtle interactions and dependencies among them. The Research conducted through CERIAS includes faculty from six different colleges and 20+ departments across campus.”

U.S. Cyber Consequences Unit (US-CCU).

<http://www.usccu.us/>

Focus: “An independent, non-profit (501c3) research institute. It provides assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks. It also investigates the likelihood of such attacks and examines the cost-effectiveness of possible counter-measures. Although the US-CCU aims to provide credible estimates of the costs of ordinary hacker mischief and white collar crime, its primary concern is the sort of larger scale attacks that could be mounted by criminal organizations, terrorist groups, rogue corporations, and nation states. The reports and briefings the US-CCU produces are supplied directly to the government, to entire critical infrastructure industries, and to the public. The US-CCU does not do any private or commercial work.”

University of Arizona, Management Information Systems (MIS) Department. “Artificial Intelligence Laboratory.”

<http://ai.arizona.edu/papers/papers.asp>

Focus: “The Artificial Intelligence Laboratory is an internationally-known research group of digital libraries, intelligent retrieval, collaborating computing, and knowledge management. Students associated with the AI Lab come from a variety of backgrounds, pursuing research in artificial intelligence, statistical analysis, computational linguistics, visualization techniques, and more. Located at The University of Arizona, in the Management Information Systems (MIS) Department, the Artificial Intelligence Lab is headed by Dr. Hsinchun Chen. The Lab is known for its adaptation and development of scalable and practical artificial intelligence, machine learning, statistical analysis, computational linguistics, and visualization techniques.”