Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues

Updated March 17, 2009

Congressional Research Service
https://crsreports.congress.gov
RL31787

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

This report describes the emerging areas of information operations, cybersecurity, and cyberwar in the context of U.S. national security. It also notes related policy issues of potential interest to Congress.

For military planners, the control of information is critical to military success, and communications networks and computers are of vital operational importance. The use of technology to both control and disrupt the flow of information has been generally referred to by several names: information warfare, electronic warfare, cyberwar, netwar, and Information Operations (IO). Currently, IO activities are grouped by the Department of Defense (DOD) into five core capabilities: (1) Psychological Operations, (2) Military Deception, (3) Operational Security, (4) Computer Network Operations, and (5) Electronic Warfare.

Current U.S. military doctrine for IO now places increased emphasis on Psychological Operations, Computer Network Operations, and Electronic Warfare, which includes use of non-kinetic electromagnetic pulse (EMP) weapons, and non-lethal weapons for crowd control. However, as high technology is increasingly incorporated into military functions, the boundaries between all five IO core capabilities are becoming blurred. DOD also acknowledges the existence of a cyber domain, which is similar to air, land, and sea. This new domain is the realm where military functions occur that involve manipulation of the electromagnetic spectrum. Control of the spectrum is essential to military success across all other domains. Definitions and examples of the overlapping categories of IO activity are contained in the appendixes.

This report will be updated to accommodate significant changes.

Contents

Appendixes

Contacts

Introduction

Background

Control of information has always been part of military operations, and the U.S. Strategic Command views information operations as a core military competency, with new emphasis on (1) use of electromagnetic energy, (2) cyber operations, and (3) use of psychological operations to manipulate an adversary's perceptions. Department of Defense (DOD) officials now consider cyberspace to be a domain for warfare, similar to air, space, land, and sea. A recent memo issued by the Secretary of Defense defines cyberspace as: "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[1]

This definition is consistent with the one presented in the 2008 National Military Strategy for Cyberspace Operations (NMS-CO), which is the overall guidance for all the services. A September 29, 2008, memo signed by the Deputy Secretary of Defense defines 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."

Cyberspace operations are a component of Information Operations (IO), which also includes Electronic Warfare (EW). Each service has organizations with IO and EW responsibilities: (1) the Naval Network Warfare Command (NETWARCOM) is the Navy's central operational authority for space, information technology requirements, network and information operations in support of naval forces afloat and ashore;[2] (2) the Army Reserve Information Operations Command has responsibility for conducting information operations, the U.S. Army IO Proponent is responsible for developing requirements for IO doctrine and training, and the Army Intelligence and Electronic Warfare Directorate provides testing services for Electronic Warfare;[3] and finally, (3) the Air Force has created what was to have been a major Cyber Command, but will now be a Numbered Air Force (NAF), the 24th Air Force to the Air Force Space Command, with responsibility for its portion of cyberwarfare, electronic warfare, and protection of U.S. critical infrastructure networks that support telecommunications systems, utilities, and transportation.[4]

The DOD views information itself as both a weapon and a target in warfare. In particular, Psychological Operations (PSYOP) provides DOD with the ability to rapidly disseminate persuasive information to directly influence the decision making of diverse audiences, and is seen

[1] This definition appears in an FOUO memo, for use of the entire DOD. Deputy Defense Secretary Gordon England, "Memorandum for Secretaries of the Military Departments, Subject: The Definition of 'Cyberspace,'" May 12, 2008, http://www.afei.org/documents/NewCyberspaceDefinition.pdf

[2] Naval Network Warfare Command, http://www.netwarcom.navy.mil/.

[3] United States Army Information Operations Proponent, April 2007, http://usacac.army.mil/CAC/usaiop.asp. James E. McConville, U.S. Army Information Operations: Concept and Execution, Military Intelligence Professional Bulletin, http://www.fas.org/irp/agency/army/mipb/1997-1/mcconvl.htm. U.S. Army Test and Evaluation Command, http://www.atec.army.mil/OTC%5Cwho_iewtd_is.htm.

[4] Peter Buxbaum, Air Force Explores the Next Frontier, *Government Computer News*, February 19, 2007, http://www.gcn.com/print/26_04/43153-1.html.

as a means for deterring aggression, and important for undermining the leadership and popular support for terrorist organizations.[5]

However, a 2006 report by the RAND Corporation describes how IO can also affect audiences outside of the intended target, stating,

> ... in contingencies involving an opponent, information operations planning and execution should include noncombatant considerations that may have nothing to do with affecting the enemy's activities or defending friendly force capabilities. In today's conflict environment the impact of information operations is seldom limited to two opposing sides. Second and higher-order effects will most likely influence all parties in opposition, impact various and varied noncombatant groups, and be interpreted in different ways by members of the media and audiences worldwide.[6]

Thus, new technologies for military IO also create new national security policy issues, including (1) consideration of psychological operations used to affect friendly nations or domestic audiences; and (2) possible accusations against the U.S. of war crimes if offensive military computer operations or electronic warfare tools severely disrupt critical civilian computer systems, or the systems of non-combatant nations.

Because of the new communications technologies and the growth of the Internet, EW and IO have taken on new importance. Insurgents use cell phones, garage door openers, and other remotely controlled electronic devices to detonate roadside bombs, and afterwards transmit video images of successful attacks against U.S. troops for broadcast on the local news or the Internet to influence public opinion about the future outcome of the war. In some cases, populations may have these video broadcasts or local TV news stories in their native language as their only source of information. DOD is seeking methods to counter these actions where violence may be seen as secondary to the use and manipulation of information.

This report describes current adversary threats in the information environment and DOD capabilities for conducting military information operations, gives the current state of federal cybersecurity efforts, and provides an overview of related policy issues.

Information Operations by Adversaries

The electromagnetic spectrum is the arena in which information operations take place. Aspects of the electromagnetic spectrum can be used by adversaries to conduct kinetic attacks, disrupt access, influence targets, and steal data. A review of the types of activity currently being conducted by adversaries illustrates the overlap between the various pillars of information operations. The following are examples of current threats to the United States.

Electronic Warfare

The US military's dominance of the electromagnetic spectrum is being challenged. Terrorist groups use wireless electronics to detonate roadside bombs (Improvised Explosive Devices).

[5] DOD Information Operations Roadmap, October 30, 2004, p. 3. This document was declassified January 2006, and obtained through FOIA by the National Security Archive at George Washington University, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

[6] Russell Glenn, *Heavy Matter: Urban Operations' Density of Challenges*, Rand Monograph Report, Turning Density to Advantage: C4ISR and Information Operations as Examples, Ch. 4, p. 25, http://www.rand.org/pubs/monograph_reports/MR1239/MR1239.ch4.pdf.

They also use the Internet to transmit financial transactions, and use free Global Positioning System (GPS) signals and commercial satellite video and images to direct their ground attacks against U.S. and coalition troops.[7] In addition, peer competitors are focusing on electronic warfare as a crucial element of their military operations by attempting to deny US forces' access to the spectrum, which enables such equipment as radars, communication links, computer networks, and sensors to work.[8]

Psychological Operations

In what some have termed the "Battle of Ideas," electronic media plays an important role in influencing populations. Reportedly, only a small portion of the Iraqi populace watch and listen to the current government run television and radio news broadcasts, with the majority preferring instead to support the foreign satellite news stations such as Al-Jazeera and Al-Arabiya. Observers say that most Arabs believe that U.S. sponsored news broadcasts are managed too closely by the coalition powers and do not objectively present the news. When the Iraqi Governing Council (IGC) prohibited Al-Jazeera and Al-Arabiya from covering all IGC events during a short period in early 2004, this action reportedly gave many Iraqi people the impression that the Coalition Provisional Authority (CPA) was manipulating their information.[9]

Some observers have also stated that terrorist groups, through use of the Internet, are now challenging the monopoly over mass communications that both state-owned and commercial media have long exercised. A strategy of the terrorists is to propagate their messages quickly and repeat them until they have saturated cyberspace. Internet messages by terrorist groups have become increasingly sophisticated through use of a cadre of Internet specialists who operate computer servers worldwide. Other observers have also stated that al-Qaeda has relied on a Global Islamic Media Unit to assist with its public outreach efforts.[10]

Computer Network Operations

As Vice Chairman of the Joint Chiefs of Staff James Cartwright told Congress in March 2007 "America is under widespread attack in cyberspace." The low cost of entry (for example, a laptop connected to the Internet), and the ability to operate anonymously, are factors that makes information operations in cyberspace attractive to adversaries who know they cannot challenge the United States in a symmetrical war. Cyber-based threats against U.S. information infrastructures are now a growing area of concern for national security. The US CERT recently revealed that attacks on US government systems increased by 40% in 2008.[11] Assaults on these systems have been sustained for nearly a decade.

In 1999, a series of attacks with the US codename "Moonlight Maze" were aimed at DOD's unclassified Non-Classified Internet Protocol Router Network (NIPRnet), the network which is used to exchange information internally. These attacks may have compromised massive amounts of sensitive military data, and appeared to originate from a mainframe in Russia. In 2003, a series

[7] Daniel Helmer, *The Poor Man's FBCB2: R U Ready 4 the 3G Celfone?*, Armor, November/December 2006, p. 7.

[8] Association of Old Crows, *Electronic Warfare: The Changing Face of Combat*, AOC The Electronic Warfare & Information Operations Association, 2009.

[9] Maj. Patrick Mackin, *Information Operations and the Global War on Terror: The Joint Force Commander's Fight for Hearts and Minds in the 21st Century*, Joint Military Operations Department, Naval War College, September 2, 2004, p. 14.

[10] Jacquelyn S. Porth, *Terrorists Use Cyberspace as Important Communications Tool*, U.S. Department of State, USInfo.State.Gov, May 5, 2006, http://usinfo.state.gov/is/Archive/2006/May/08-429418.html.

[11] Peter Eisler, "Reported Raids on Federal Computer Data Soar," *USA Today*, February 17, 2009.

of cyberattacks designed to copy sensitive data files was launched against DOD systems, and the computers belonging to DOD contractors. The cyberespionage attack apparently went undetected for many months. This series of cyberattacks was labeled "Titan Rain," and was suspected by DOD investigators to have originated in China. The attacks were directed against the U.S. Defense Information Systems Agency (DISA), the U.S. Redstone Arsenal, the Army Space and Strategic Defense Installation, and several computer systems critical to military logistics. Although no classified systems reportedly were breached, many files were copied containing information that is sensitive and subject to U.S. export-control laws.

In 2006, an extended cyberattack against the U.S. Naval War College in Newport, Rhode Island, prompted officials to disconnect the entire campus from the Internet.[12] A similar attack against the Pentagon in 2007 led officials to temporarily disconnect part of the unclassified network from the Internet. DOD officials acknowledge that the Global Information Grid, which is the main network for the U.S. military, experiences more than three million daily scans by unknown potential intruders.[13]

Lt. General Charles Croom (JTF-Global Net Operations) has stated that cyber attackers "are not denying, disrupting, or destroying [American military] operations – yet. But that doesn't mean they don't have the capability."[14] Potential adversaries, such as China, Russia, Cuba, Iran, Iraq, Libya, North Korea, and several non-state terrorist groups are reportedly developing capabilities to attack or degrade U.S. civilian and military networks. "Titan Rain" is an example of successful attacks against non-classified military systems which DOD officials claim were directed by other governments.[15] Maj. Gen. William Lord (Air Force) stated publicly in 2007 that "China has downloaded 10 to 20 terabytes of data from the NIPRNet already."

According to the Defense Department's annual report to Congress on China's military prowess, the Chinese military is enhancing its information operations capabilities.[16] The report finds that China is placing specific emphasis on the ability to perform information operations designed to weaken an enemy force's command and control systems.[17]

Cyberwarfare: Estonia, Georgia and Kyrgystan

On April 27, 2007, officials in Estonia moved a Soviet-era war memorial commemorating an unknown Russian who died fighting the Nazis. The move stirred emotions, inciting rioting by ethnic Russians, and the blockading of the Estonian Embassy in Moscow. The event also marked the beginning of a series of large and sustained Distributed Denial-Of-Service (DDOS) attacks launched against several Estonian national websites, including government ministries and the

[12] Chris Johnson, Naval War College Network, "Web Site Back Up Following Intrusion," *Inside the Navy*, December 18, 2006.

[13] Some estimates say that up to 90% of computer software used in China is pirated, and thus open to hijack through computer viruses. James Lewis, *Computer Espionage, Titan Rain and China*, Center for Strategic and International Studies, December 14, 2005.

[14] Rebecca Grant, *Victory in Cyberspace: An Air Force Special Report*, Air Force, October 2007.

[15] Elinor Abreu, *Epic cyberattack reveals cracks in U.S. defense*, CNN.com, May 10, 2001, http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/. Declan McCullagh, *Feds Say Fidel Is Hacker Threat*, WiredNews.com, February 9, 2001, http://www.wired.com/news/politics/0,1283,41700,00.html. Staff, *Cyberattack could result in military response*, USAToday, February 14, 2002, http://www.usatoday.com/tech/news/2002/02/14/cyberterrorism.htm.

[16] See the FY2004 Report to Congress on PRC Military Power, http://www.defenselink.mil/pubs/d20040528PRC.pdf.

[17] John Bennett, "Commission: U.S. Should Push Beijing to up Pressure on North Korea," *Inside the Pentagon*, June 17, 2004.

prime minister's Reform Party.[18] DDOS attacks occur when remote computers, often vast networks of "zombies" infected with malicious code, are instructed to target particular websites with requests, overwhelming the sites with traffic so that they become unavailable. Estonia's infrastructure relies heavily on information technology, and the country is described as being the most "wired" in Europe. Because availability of basic services to Estonian citizens was disrupted, the attacks were considered crippling.

Initially, the Russian government was blamed by Estonian officials for the cyberattacks, but it is unclear whether the attacks are sanctioned or initiated by the Russian government. NATO sent computer security experts to Estonia to help protect government systems against continued attacks, and to help recover from the attacks.

However, some analysts later concluded that the cyber attacks targeting Estonia were not a concerted attack, but instead were the product spontaneous anger from a loose federation of separate attackers. Technical data showed that sources of the attack were worldwide rather than concentrated in a few locations. The computer code that caused the DDOS attack was posted and shared in many Russian language chat rooms, where the moving of the statue was a very emotional topic for discussion. These analysts state that although various Estonian government agencies were taken offline, there was no apparent attempt to target national critical infrastructure other than internet resources, and no extortion demands were made. Their analysis concluded that there was no Russian government connection to the attacks against Estonia.[19]

Occurring simultaneously with a kinetic attack by Russian forces on Georgia's separatist regions, the country's major internet service providers were targeted with coordinated, sustained cyber attacks, knocking the some of the government's websites offline while defacing others. Investigations later determined that the attacks began with online Russian hacking forums, who distributed lists of Georgian internet sites as targets. Unlike the DDOS attacks on Estonia, the Georgian sites were taken down by exploiting a vulnerability in widely used software to manage Web databases. Rather than involving botnets comprised of thousands, attacks of this nature can be conducted with a single computer. In its effort to mitigate the attacks, the Georgian government blocked all internet traffic originating from Russian users. However, blogs quickly appeared with detailed instructions on how to bypass the block by re-routing the traffic through internet addresses in other countries.[20]

Although there is no evidence linking the Russian government directly, there is much to suggest that the attacks were at least tolerated and perhaps even encouraged by Russian officials.

In another example of the growing popularity of cyber attacks as an intimidation tactic, Kyrgystan's two main internet service providers—which take up approximately 80% of the country's bandwidth—were systematically targeted with denial of service attacks, effectively taking the country offline. Again, there is no evidence of direct involvement with the Russian Government; these attacks instead appeared to have originated with a Russian "cyber militia."[21] Possible motives for the network assault include Russia's displeasure with a U.S. air base located in Kyrgystan, and with the Kyrzyg government's opposition party, which relies on the internet as its media outlet.

---

[18] Robert Vamosi, *Cyberattack in Estonia—what it really means*, CnetNews.com, May 29, 2007, http://news.com.com/Cyberattack+in+Estonia-what+it+really+means/2008-7349_3-6186751.html.

[19] *Estonian DDoS—a final analysis*, Heise Security, http://www.heise-security.co.uk/news/print/90461.

[20] Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html

[21] "Kyrgystan Knocked Offline" *Wall Street Journal*, January 28, 2009, pg. 10.

A persistent problem after a computer network attack is accurate and timely identification of the attacker. This uncertainty may affect decisions about how and against whom, or even whether, to retaliate.

Law and Proportionality for Information Operations

These incidents indicate a trend towards cyberattacks as a form of political manipulation. If cyberspace is a new battlefield on which war may be waged, then the international community will be challenged to come together to determine its conduct. The attack on Estonia, a member of NATO, raised questions of whether the actions taken could be defined as an "armed attack" under Article 5 of the Washington Treaty.[22] Internationally, Article 51 of the Charter of the United Nations is the guidance for response.[23] For now, NATO and other states consider network protection to be a national responsibility. However, questions of sovereignty, attribution, and response thresholds remain.

It has been presumed that the rules of engagement for information operations will follow the law of Armed Conflict, meaning a response taken after receiving an electronic or cyber attack will be scaled in proportion to the attack received, and distinctions will be maintained between combatants and civilians.[24] However, protection against attack through cyberspace is a new task for the military, and the offensive tools and other capabilities used by DOD to stage retaliatory strikes against enemy systems are highly classified. Experience has shown that a reactive defense is not very effective against increasingly powerful and rapid malicious cyber attacks, or against other malicious activity using the electromagnetic spectrum. A more effective defense against these attacks is to incorporate predictive, active, and pre-emptive measures that allow DOD defenders to prevent, deflect, or minimize the efforts of the attacker.

Accurate attribution is important when considering whether to retaliate using military force or police action. Some DOD officials have indicated that the majority of cyber attacks against DOD and U.S. civilian agency systems are suspected to originate in China, and these attacks are consistently more numerous and sophisticated than cyberattacks from other malicious actors. The motives appear to be primarily cyberespionage against civilian agencies, DOD contractors, and DOD systems. The espionage involves unauthorized access to files containing sensitive industrial technology, and unauthorized research into DOD operations. Some attacks included attempts to implant malicious code into computer systems for future use by intruders.[25]

---

[22] Article V states that an armed attack against one member shall be considered an attack against them all, and that if such an attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party with such action as it deems necessary, including the use of armed force. Full text of the Washington Treaty is available at http://www.nato.int/docu/basictxt/treaty.htm.

[23] Chapter VII, *Actions With Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*. Article 51 of the UN Charter recognizes the members' rights to self-defense in the event of an armed attack.

[24] The Law of Armed Conflict (LOAC) is a part of public international law that regulates the conduct of armed hostilities between nations, and is intended to protect civilians, the wounded, sick, and shipwrecked. LOAC training for U.S. military is a treaty obligation for the United States under provisions of the 1949 Geneva Conventions. Also, under 18 U.S. Code 2441, war crimes committed by or against Americans may violate U.S. criminal law. James Baker, *When Lawyers Advise Presidents in Wartime,* Naval War College Review, Winter 2002, Vol. LV, No. 1. Terry Kiss, ed., Law of Armed Conflict, Air University Library, Maxwell AFB, Jan 2005, http://www.au.af.mil/au/aul/bibs/loacots.htm.

[25] Josh Rogin, "Cyber officials: Chinese hackers attack 'anything and everything,'" FCW.com, February 13, 2007, http://www.fcw.com/article97658-02-13-07-Web&printLayout.

Cyberattack, Cybercrime, and Cyberterrorism

In order to determine the legality of a response to malicious cyber behavior, the categories of activity, actors, and jurisdictions must be clearly defined. Labeling a "cyberattack" as "cybercrime" or "cyberterrorism" is problematic because of the difficulty determining with certainty the identity, intent, or the political motivations of an attacker.[26] "Cybercrime" can be very broad in scope, and may sometimes involve more factors than just a computer hack. "Cyberterrorism" is often equated with the use of malicious code. However, a "cyberterrorism" event may also sometimes depend on the presence of other factors beyond just a "cyberattack."

Cyberterrorism

Various definitions exist for the term "cyberterrorism," just as various definitions exist for the term "terrorism."[27] Analysis of cyberspace misconduct is complicated by the presence of violence in the definitions of terrorism. Security expert Dorothy Denning defines cyberterrorism as "... politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage."[28] The Federal Emergency Management Agency (FEMA) defines cyberterrorism as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[29]

Others indicate that a physical attack that destroys computerized nodes for critical infrastructures, such as the Internet, telecommunications, or the electric power grid, without ever touching a keyboard, can also contribute to, or be labeled as cyberterrorism.[30] Thus, it is possible that if a computer facility were deliberately attacked for political purposes, all three methods described above (physical attack, EA, and cyberattack) might contribute to, or be labeled as "cyberterrorism."

CRS is unaware of any reported acts of cyberterrorism, to date.

Cybercrime

Cybercrime is crime that is enabled by, or that targets computers. Some argue there is no agreed-upon definition for "cybercrime" because "cyberspace" is just a new specific instrument used to help commit crimes that are not new at all. Cybercrime can involve theft of intellectual property, a violation of patent, trade secret, or copyright laws. However, cybercrime also includes attacks against computers to deliberately disrupt processing, or may include espionage to make unauthorized copies of classified data. If a terrorist group were to launch a cyberattack to cause

[26] Serge Krasavin, *What is Cyberterrorism?* Computer Crime Research Center, April 23, 2004, http://www.crime-research.org/analytics/Krasavin/.

[27] Under 22 USC, Section 2656, "terrorism" is defined as premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents, usually intended to influence an audience. The United States has employed this definition of terrorism for statistical and analytical purposes since 1983. U.S. Department of State, 2002, *Patterns of Global Terrorism, 2003*, http://www.state.gov/s/ct/rls/pgtrpt/2001/html/10220.htm.

[28] Dorothy Denning, "Activism, Hactivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, eds., *Networks and Netwars*, (Rand 2001), p. 241. Dorothy Denning, *Is Cyber War Next?* Social Science Research Council, November 2001, at http://www.ssrc.org/sept11/essays/denning.htm.

[29] http://www.fema.gov/pdf/onp/toolkit_app_d.pdf.

[30] Dan Verton, "A Definition of Cyber-terrorism," *Computerworld*, August 11, 2003, http://www.computerworld.com/securitytopics/security/story/0,10801,83843,00.html.

harm, such an act also fits within the definition of a cybercrime. The primary difference between a cyberattack to commit a crime or to commit terror is found in the intent of the attacker, and it is possible for actions under both labels to overlap.

One of the most prevalent forms of cybercrime is identity theft. Botnets and other examples of malicious code can operate to assist cybercriminals with identity theft, a crime generally motivated by financial gain. Current FBI estimates are that identity theft costs American businesses and consumers $50 billion a year. Individual users are often lured into clicking on tempting links that are found in email or when visiting websites. Clicking on titles such as "Buy Rolex watches cheap," or "Check out my new Photos," can take advantage of web browser vulnerabilities to place malicious software onto a users system which allows a cybercriminal to gather personal information from the user's computer.

Malicious code can scan a victim's computer for sensitive information, such as name, address, place and date of birth, social security number, mother's maiden name, and telephone number. Full identities obtained this way are bought and sold in online markets. False identity documents can then be created from this information using home equipment such as a digital camera, color printer, and laminating device, to make official-looking driver's licenses, birth certificates, reference letters, and bank statements.[31]

Identity theft involving thousands of victims is also enabled by inadequate computer security practices within organizations.[32] MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to U.S. consumers were accessed by computer hackers.[33] Some of these account numbers were reportedly being sold on a Russian website, and some consumers have reported fraudulent charges on their statements. Officials at the UFJ bank in Japan reportedly stated that some of that bank's customers may also have become victims of fraud related to theft of the MasterCard information.[34] In June 2006, officials from the U.S. Department of Energy acknowledged that names and personal information belonging to more than 1,500 employees of the National Nuclear Security Administration (NNSA) had been stolen in a network intrusion that apparently took place starting in 2004. The NNSA did not discover the security breach until one year after it had occurred.[35]

Some sources report that stolen credit card numbers and bank account information are traded online in a highly structured arrangement, involving buyers, sellers, intermediaries, and service industries. Services include offering to conveniently change the billing address of a theft victim, through manipulation of stolen PINs or passwords. Observers estimated that in 2005 such

[31] Lou Bobson, "Identity Theft Ruining Lives," *The Sunday Mail*, May 20, 2007, p. 62.

[32] On April 12, 2005, personal information, such as Social Security Numbers for 310,000 U.S. citizens, may have been stolen in a data security breach that involved 59 instances of unauthorized access into its corporate databases using stolen passwords. Boston College reported in March 2005 that a hacker had gained unauthorized access to computer database records with personal information for up to 106,000 alumni, and in the same month, Chico State University of California, reported that its databases had been breached containing the names and Social Security numbers for as many as 59,000 current and former students. David Bank and Christopher Conkey, "New Safeguards for Your Privacy," *The Wall Street Journal*, March 24, 2005, p. D1.

[33] Jonathan Krim and Michael Barbaro, "40 Million Credit Card Numbers Hacked," *Washington Post*, June 18, 2005, p. A01. See also the report by the U.S. House of Representatives Homeland Security Committee, July 1, 2005, raising concerns about potential ties between identity theft victims and terrorism. Caitlin Harrington, "Terrorists Can Exploit Identity Theft, Report From House Democrats Says," *CQ Homeland Security*, July 1, 2005.

[34] BBC News, "Japan Cardholders 'Hit' by Theft," June 21, 2005, at http://news.bbc.co.uk/1/hi/business/4114252.stm.

[35] Dawn Onley and Patience Wait, "DOD's Efforts to Stave off Nation-State Cyberattacks Begin with China," *Government Computer News*, August 21, 2006.

services for each stolen MasterCard number cost between $42 and $72.[36] Other news articles report that, in 2007, a stolen credit card number sells online for only $1, and a complete identity, including a U.S. bank account number, credit-card number, date of birth, and a government-issued ID number now sells for just $14 to $18.[37]

As of January 2007, 35 states have enacted data security laws requiring businesses that have experienced an intrusion involving possible identity theft to notify persons affected, and to improve security for protection of restricted data. However, existing federal and state laws that impose obligations on information owners, may require harmonization to provide protections that are more uniform.[38]

Identity theft continues to plague government systems. The U.S. government's online recruiting website, monster.com, suffered an intrusion in August 2007 that affected the confidential information of nearly 1.3 million users. The company admitted to waiting several days before notifying the public of the breach. The website was attacked again in February 2009, resulting in the theft of personal data for millions of users worldwide. In February 2009, the Federal Aviation Administration issued a letter exposing a data breach that affected more than 45,000 employees. There have been many criticisms of the FAA's handling of the situation, particularly for its failure to publish pertinent information on its website. Some argue that FISMA's requirements have agencies focused on meeting deadlines rather than expending resources on added security measures.

Also in February 2009, the Air Force shut down all internet access at Maxwell Air Force Base, Alabama. The measure was in response to an intrusion that may have affected the security of all Air Force systems, but also to stress the importance of information assurance to individual components. Air Force Chief of Staff General Schwartz stated that the disconnect was ordered because personnel *"hadn't demonstrated—in our view at the headquarters—their capacity to manage their network in a way that didn't make everyone else vulnerable. This is the kind of effort that's required up and down the line."*

On March 10, 2009, the Army publicly announced a breach of a database containing personal information about nearly 1,600 soldiers. The intrusions may have compromised the data on those participating in the Army's Operation Tribute to Freedom program, which allows soldiers to share their stories with the public. (For details on cybercrime and federal computer fraud, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

Cyberespionage

Cyberespionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing, copying, and exfiltration of data files. Deliberate network intrusions, whether for industrial espionage or espionage involving military information, qualify as cyberespionage. If there is disagreement about this, it is likely because technology has outpaced policy for labeling actions in cyberspace. In fact, industrial cyberespionage may now be considered a necessary part of global economic competition, and

[36] CCRC staff, *Russia, Biggest Ever Credit Card Scam*, Computer Crime Research Center, July 8, 2005, at http://www.crime-research.org/news/08.07.2005/1349/.

[37] David Hayes, "A Dollar goes a Long Way in Swiping Private Data," *The Kansas City Star*, March 20, 2007, p. 1.

[38] For more information about laws related to identity theft, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Marie Stevens.

secretly monitoring the computerized functions and capabilities of potential adversary countries may also be considered essential for national defense.[39]

U.S. counterintelligence officials reportedly have stated that about 140 different foreign intelligence organizations regularly attempt to hack into the computer systems of U.S. government agencies and U.S. companies. Cyberespionage, which enables the extraction of massive amounts of information electronically, has now transformed the nature of counterintelligence, by enabling a reduced reliance on conventional spying operations.[40] The Internet, including satellite links and wireless local networks, now offers new, low cost and low risk opportunities for espionage. In 2001, a Special Committee of Inquiry established by the European Parliament accused the United States of using its Echelon electronic spy network to engage in industrial espionage against European businesses. Echelon was reportedly set up in 1971 as an electronic monitoring system during the Cold War. European Union member Britain operates the system, which includes listening posts in Canada, Australia, and New Zealand. Echelon is described as a global spy system reportedly capable of intercepting wireless phone calls, e-mail, and fax messages made from almost any location around the world.[41]

Former director of the U.S. Central Intelligence Agency, James Woolsey, has reportedly justified the possibility of industrial espionage by the United States on the basis of the use of bribery by European companies. Officials of the European parliament reportedly expressed outrage about the justification, while not denying that bribery is sometimes used to make sales.[42]

Some government officials warn that criminals now sell or rent malicious code tools for cyberespionage, and the risk for damage to U.S. national security due to cyberespionage conducted by other countries is great. One industry official, arguing for stronger government agency computer security practices, stated that, "If gangs of foreigners broke into the State or Commerce Departments and carried off dozens of file cabinets, there would be a crisis. When the same thing happens in cyberspace, we shrug it off as another of those annoying computer glitches we must live with."[43]

Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some malicious actors consider that no boundaries exist between military and civilian targets. According to an August 2005 computer security report by IBM, more than 237 million overall

[39] U.S. intelligence officials, speaking on background, explained that they have routinely penetrated potential enemies' computer networks. These officials claim that thousands of attacks have taken place and sensitive information was stolen. John Stanton, "Rules of Cyber War Baffle U.S. Government Agencies," *National Defense*, February 2000, http://www.nationaldefensemagazine.org/issues/2000/Feb/Rules.htm.

[40] Jeanne Meserve, "Official: International Hackers Going after U.S. Networks," CNN.com, October 19, 2007, http://www.cnn.com/2007/US/10/19/cyber.threats/index.html.

[41] Martin Asser, "Echelon: Big brother without a cause?" BBC News, July 6, 2000, http://news.bbc.co.uk/1/hi/world/europe/820758.stm.

[42] European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), European Parliament approved on September 5, 2001, by 367 votes for, 159 against, and 39 abstentions, http://www.cyber-rights.org/interception/echelon/European_parliament_resolution.htm. Gerhard SCHMID *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*, Doc.: A5-0264/2001, May 9, 2001, http://www.statewatch.org/news/2001/sep/02echelon.htm. James Woolsey, *Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage*, Federation of American Scientists, March 7, 2000, http://ftp.fas.org/irp/news/2000/03/wool0300.htm.

[43] James Lewis, testimony before the House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, April 15, 2007.

security attacks were reported globally during the first half of that year.[44] Government agencies were targeted the most, reporting more than 54 million attacks, while manufacturing ranked second with 36 million attacks, financial services ranked third with approximately 34 million, and healthcare received more than 17 million attacks. The most frequent targets for these attacks, all occurring in the first half of 2005, were government agencies and industries in the United States (12 million), followed by New Zealand (1.2 million), and China (1 million). These figures likely represent an underestimation, given that most security analysts agree that the number of incidents reported are only a small fraction of the total number of attacks that actually occur.

Terrorism Linked to Cybercrime

The proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. However, linkages do exist between terrorist groups and criminals that allow terror networks to expand internationally through leveraging the computer resources, money laundering activities, or transit routes operated by criminals. For example, the 2005 U.K. subway and bus bombings, and the attempted car bombings in 2007, also in the U.K., provide evidence that groups of terrorists are already secretly active within countries with large communication networks and computerized infrastructures, plus a large, highly skilled IT workforce. London police officials reportedly believe that terrorists obtained high-quality explosives used for the 2005 U.K. bombings through criminal groups based in Eastern Europe.[45]

A recent trial in the U.K. revealed a significant link between Islamic terrorist groups and cybercrime. In June 2007, three British residents, Tariq al-Daour, Waseem Mughal, and Younes Tsouli, pled guilty, and were sentenced for using the Internet to incite murder. The men had used stolen credit card information at online web stores to purchase items to assist fellow jihadists in the field—items such as night vision goggles, tents, global positioning satellite devices, and hundreds of prepaid cell phones, and more than 250 airline tickets, through using 110 different stolen credit cards. Another 72 stolen credit cards were used to register over 180 Internet web domains at 95 different web hosting companies. The group also laundered money charged to more than 130 stolen credit cards through online gambling websites. In all, the trio made fraudulent charges totaling more than $3.5 million from a database containing 37,000 stolen credit card numbers, including account holders' names and addresses, dates of birth, credit balances, and credit limits.[46]

Cybercriminals have made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where illegal drug funds or other profitable activities such as credit card theft, are used to support terrorist groups.[47] Drug traffickers are reportedly among the most widespread users of encryption for Internet messaging, and are able to hire high-level computer specialists to help evade law enforcement, coordinate shipments of drugs, and launder money. Regions with major

[44] The Global Business Security Index reports worldwide trends in computer security from incidents that are collected and analyzed by IBM and other security organizations. IBM press release, *IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005*, IBM, August 2, 2005.

[45] Walsh, *Terrorism on the Cheap*. Rollie Lal, "Terrorists and Organized Crime Join Forces," *International Herald Tribune*, May 25, 2005, at http://www.iht.com/articles/2005/05/23/opinion/edlal.php. Barbara Porter, "Forum Links Organized Crime and Terrorism," *By George!* summer 2004 http://www2.gwu.edu/~bygeorge/060804/crimeterrorism.html.

[46] Brian Krebs, "Three Worked the Web to Help Terrorists," *The Washington Post*, July 6, 2007, p. D01.

[47] Peter Bergen, "The Taliban, Regrouped and Rearmed," *The Washington Post*, September 10, 2006, p. B1. Helen Cooper, "NATO Chief Says More Troops Are Needed in Afghanistan," *The New York Times*, September 22, 2006, p. 10.

narcotics markets, such as Western Europe and North America, also possess optimal technology infrastructure and open commercial nodes that increasingly serve the transnational trafficking needs of both criminal and terrorist groups.[48] Officials of the U.S. Drug Enforcement Agency (DEA), reported in 2003 that 14 of the 36 groups found on the U.S. State Department's list of foreign terrorist organizations were also involved in drug trafficking. A 2002 report by the Federal Research Division at the Library of Congress, revealed a "growing involvement of Islamic terrorist and extremists groups in drug trafficking," and limited evidence of cooperation between different terrorist groups involving both drug trafficking and trafficking in arms.[49] Consequently, DEA officials reportedly argued that the war on drugs and the war against terrorism are and should be linked.[50]

State Department officials, at a Senate hearing in March 2002, also indicated that some terrorist groups may be using drug trafficking as a way to gain financing while simultaneously weakening their enemies in the West through exploiting their desire for addictive drugs.[51] The poppy crop in Afghanistan reportedly supplies resin to produce over 90% of the world's heroin, supporting a drug trade estimated at $3.1 billion. Reports indicate that money from drug trafficking in Afghanistan is used to help fund terrorist and insurgent groups that operate in that country. Subsequently, U.S. intelligence reports in 2007 have stated that "al Qaeda in Afghanistan" has been revitalized and restored to its pre-September 11, 2001 operation levels, and may now be in a better position to strike Western countries.[52]

Drug traffickers have the financial clout to hire computer specialists with skills for using technologies which make Internet messages hard or impossible to decipher, and which allow terrorist organizations to transcend borders and operate internationally with less chance of detection. Many highly trained technical specialists that make themselves available for hire originally come from the countries of the former Soviet Union and the Indian subcontinent. Some of these technical specialists reportedly will not work for criminal or terrorist organizations willingly, but may be misled or unaware of their employers' political objectives. Still, others will agree to provide assistance because other well-paid legitimate employment is scarce in their region.[53]

---

[48] Glenn Curtis and Tara Karacan, *The Nexus Among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe*, a study prepared by the Federal Research Division, Library of Congress, December 2002, p. 22, at http://www.loc.gov/rr/frd/pdf-files/WestEurope_NEXUS.pdf.

[49] L. Berry, G.E. Curtis, R.A. Hudson, and N. A. Kollars, *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups*, Federal Research Division, Library of Congress, Washington, DC, May 2002.

[50] Authorization for coordinating the federal war on drugs expired on September 30, 2003. For more information, see CRS Report RL32352, *War on Drugs: Reauthorization and Oversight of the Office of National Drug Control Policy*, by Mark Eddy. Also, see D.C. Préfontaine, QC and Yvon Dandurand, *Terrorism and Organized Crime Reflections on an Illusive Link and its Implication for Criminal Law Reform*, International Society for Criminal Law Reform Annual Meeting—Montreal, August 8-12, Workshop D-3 Security Measures and Links to Organized Crime, August 11, 2004, at http://www.icclr.law.ubc.ca/Publications/Reports/International%20Society%20Paper%20of%20Terrorism.pdf.

[51] Rand Beers and Francis X. Taylor, U.S. State Department, *Narco-Terror: The Worldwide Connection Between Drugs and Terror*, testimony before the U.S. Senate Judiciary Committee, Subcommittee on Technology, Terrorism, and Government Information, March 13, 2002.

[52] Matthew Lee and Katherine Shrader, *Al-Qaida has rebuilt, U.S. intel warns*, Associated Press, July 12, 2007, http://news.yahoo.com/s/ap/20070712/ap_on_go_pr_wh/us_terror_threat_32;_ylt=AuURr2eP8AhBrfHyTOdw714Gw_IE. Associated Press, "Afghanistan's poppy crop could yield more than 2006's record haul, UN says," International Herald Tribune, June 25, 2007, http://www.iht.com/articles/ap/2007/06/25/asia/AS-GEN-Afghan-Drugs.php.

[53] Louise Shelly, *Organized Crime, Cybercrime and Terrorism*, Computer Crime Research Center, September 27, 2004, http://www.crime-research.org/articles/Terrorism_Cybercrime/.

Terrorist Groups Linked to Hackers

Links between computer hackers and terrorists, or terrorist-sponsoring nations may be difficult to confirm. Membership in the most highly skilled computer hacker groups is sometimes very exclusive and limited to individuals who develop, demonstrate, and share only with each other, their most closely guarded set of sophisticated hacker tools. These exclusive hacker groups do not seek attention because maintaining secrecy allows them to operate more effectively. Some hacker groups may also have political interests that are supra-national, or based on religion, or other socio-political ideologies, while other hacker groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer services, regardless of the political interests involved.

Information about computer vulnerabilities is now for sale online in a hackers' "black market." For example, a list of 5,000 addresses of computers that have already been infected with spyware and which are waiting to be remotely controlled as part of an automated "bot network" reportedly can be obtained for about $150 to $500. Prices for information about computer vulnerabilities for which no software patch yet exists reportedly range from $1,000 to $5,000. Purchasers of this information are often organized crime groups, various foreign governments, and companies that deal in spam.[54]

Terrorist Capabilities for Cyberattack

Some experts estimate that advanced or structured cyberattacks against multiple systems and networks, including target surveillance and testing of sophisticated new hacker tools, might require from two to four years of preparation, while a complex coordinated cyberattack, causing mass disruption against integrated, heterogeneous systems may require 6 to 10 years of preparation.[55] This characteristic, where hackers devote much time to detailed and extensive planning before launching a cyberattack, has also been described as a "hallmark" of previous physical terrorist attacks and bombings launched by Al Qaeda.

It is difficult to determine the level of interest, or the capabilities of international terrorist groups to launch an effective cyberattack. A 1999 report by The Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School concluded that it is likely that any severe cyberattacks experienced in the near future by industrialized nations will be used by terrorist groups simply to supplement the more traditional physical terrorist attacks.[56]

Some observers have stated that Al Qaeda does not see cyberattack as important for achieving its goals, preferring attacks which inflict human casualties.[57] Other observers believe that the groups most likely to consider and employ cyberattack and cyberterrorism are the terrorist groups operating in post-industrial societies (such as Europe and the United States), rather than

[54] Hackers sell their information anonymously through secretive websites. Bob Francis, "Know Thy Hacker," *Infoworld*, January 28, 2005 at http://www.infoworld.com/article/05/01/28/05OPsecadvise_1.html.

[55] Dorothy Denning, "Levels of Cyberterror Capability: Terrorists and the Internet," http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt, presentation, and Zack Phillips, "Homeland Tech Shop Wants to Jump-Start Cybersecurity Ideas," *CQ Homeland Security*, September 14, 2004 at http://homeland.cq.com/hs/display.do?docid=1330150&sourcetype=31&binderName=news-all.

[56] Report was published in 1999, available at http://www.nps.navy.mil/ctiw/reports/.

[57] The Ashland Institute for Strategic Studies has observed that Al Qaeda is more fixated on physical threats than electronic ones. John Swartz, "Cyberterror Impact, Defense Under Scrutiny," *USA Today*, August 3, 2004, p. 2B.

international terrorist groups that operate in developing regions where there is limited access to high technology.

However, other sources report that Al Qaeda has taken steps to improve organizational secrecy through more active and sophisticated use of technology, and evidence suggests that Al Qaeda terrorists used the Internet extensively to plan their operations for September 11, 2001.[58] In past years, Al Qaeda groups reportedly used new Internet-based telephone services to communicate with other terrorist cells overseas. Khalid Shaikh Mohammed, one of the masterminds of the attack against the World Trade Center, reportedly used special Internet chat software to communicate with at least two airline hijackers. Ramzi Yousef, who was sentenced to life imprisonment for the previous bombing of the World Trade Center, had trained as an electrical engineer, and had planned to use sophisticated electronics to detonate bombs on 12 U.S. airliners departing from Asia for the United States. He also used sophisticated encryption to protect his data and to prevent law enforcement from reading his plans should he be captured.[59]

Tighter physical security measures now widely in place throughout the United States may encourage terrorist groups in the future to explore cyberattack as way to lower the risk of detection for their operations.[60] However, other security observers believe that terrorist organizations might be reluctant to launch a cyberattack because it would result in less immediate drama and have a lower psychological impact than a more conventional bombing attack. These observers believe that unless a cyberattack can be made to result in actual physical damage or bloodshed, it will never be considered as serious as a nuclear, biological, or chemical terrorist attack.[61] Some experts fear that an attack on critical infrastructures such as the nation's electric grid or Supervisory Control and Data Acquisition (SCADA) utilities delivery systems, either through kinetic or cyber means, may be more likely. (For an explanation of vulnerabilities and security measures, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.)

International Convention on Cybercrime

Cybercrime is also a major international challenge, even though attitudes about what comprises a criminal act of computer wrongdoing still vary from country to country. However, the Convention on Cybercrime was adopted in 2001 by the Council of Europe, a consultative assembly of 43 countries, based in Strasbourg. The Convention, effective July 2004, is the primary international treaty dealing with breaches of law "over the internet or other information networks." The Convention requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.[62]

Although the United States has signed and ratified the Convention, it did not sign a separate protocol that contained provisions to criminalize xenophobia and racism on the Internet, which

[58] David Kaplan, "Playing Offense: The Inside Story of How U.S. Terrorist Hunters Are Going after Al Qaeda," *U.S. News & World Report*, June 2, 2003, pp. 19-29.

[59] Robert Windrem, "9/11 Detainee: Attack Scaled Back," September 21, 2003, http://www.msnbc.com/news/969759.asp.

[60] "Terrorism: An Introduction," April 4, 2003 at http://www.terrorismanswers.com/terrorism.

[61] James Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," December 2002 at http://www.csis.org/tech/0211_lewis.pdf.

[62] Full text for the Convention on Cyber Crime may be found at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=18/06/04&CL=ENG.

would raise Constitutional issues in the United States.[63] The separate protocol could be interpreted as requiring nations to imprison anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or ethnic origin, a requirement that could make it a crime to e-mail jokes about ethnic groups or question whether the Holocaust occurred. Reportedly, the Department of Justice has said that it would be unconstitutional for the United States to sign that additional protocol because of the First Amendment's guarantee of freedom of expression. The Electronic Privacy Information Center, in a June 2004 letter to the Foreign Relations Committee, objected to U.S. ratification of the Convention, because it would "create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[64]

On August 3, 2006, the U.S. Senate passed a resolution of ratification for the Convention. The United States will comply with the Convention based on existing U.S. federal law; and no new implementing legislation is expected to be required. Legal analysts say that U.S. negotiators succeeded in scrapping most objectionable provisions, thereby ensuring that the Convention tracks closely with existing U.S. laws.[65]

The Need to Improve Cybersecurity

Department of Defense (DOD) officials have stated that, while the threat of cyber attack is "less likely" to appear than conventional physical attack, it could actually prove more damaging because it could involve disruptive technology that might generate unpredictable consequences that give an adversary unexpected advantages.[66] The Homeland Security Presidential Directive 7 required that the Department of Homeland Security (DHS) coordinate efforts to protect the cybersecurity for the nation's critical infrastructure. This resulted in two reports in 2005, titled "Interim National Infrastructure Protection Plan," and "The National Plan for Research and Development in Support of Critical Infrastructure Protection," where DHS provided a framework for identifying and prioritizing, and protecting each infrastructure sector.

However, some observers question why, in light of the many such reports describing an urgent need to reduce cybersecurity vulnerabilities, there is not an apparent perceived sense of national urgency to close the gap between cybersecurity and the threat of cyberattack. For example, despite Federal Information Security Management Act of 2002 (FISMA), some experts argue that security remains a low priority, or is treated almost as an afterthought at some domestic federal agencies.[67] In 2007, the Government Accountability Office issued a report, titled "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but

[63] The U.S. Senate Committee on Foreign Relations held a hearing on the Convention on June 17, 2004. CRS Report RS21208, *Cybercrime: The Council of Europe Convention*, by Kristin Archick. Estelle Durnout, *Council of Europe Ratifies Cybercrime Treaty*, ZDNet, March 22, 2004, at http://news.zdnet.co.uk/business/legal/0,39020651,39149470,00.htm.

[64] http://www.epic.org/privacy/intl/senateletter-061704.pdf.

[65] For more information about the Convention on Cybercrime, see CRS Report RS21208, *Cybercrime: The Council of Europe Convention*, by Kristin Archick.

[66] Advantages of EA and CNA might derive from United States reliance on a computer-controlled critical infrastructure, along with unpredictable results depending on severity of the attack. Jason Sherman, "Bracing for Modern Brands of Warfare," *Air Force Times*, September 27, 2004, http://www.airforcetimes.com/story.php?f=1-AIRPAPER-358727.php.

[67] Statement of James A. Lewis, Senior Fellow and Director, Technology and Public Policy Program, Center for Strategic and International Studies, Committee on House Oversight and Government Reform Subcommittee on Government Management, Organization, and Procurement, Subcommittee on Information Policy, Census, and National Archives, June 7, 2007.

Challenges Remain," which states that cybersecurity risks have actually increased for infrastructure control systems because of the persistence of interconnections with the Internet, and continued open availability of detailed information on the technology and configuration of the control systems. The report states that no overall strategy yet exists to coordinate activities to improve computer security across federal agencies and the private sector, which owns the critical infrastructure.[68] Some observers argue that, as businesses gradually strengthen their security policies for headquarters and administrative systems, the remote systems that control critical infrastructure and manufacturing may soon be seen as easier targets of opportunity for cybercrime.

Cybercrime is obviously one of the risks of doing business in the age of the internet, but observers argue that many decision-makers may currently view it as a low-probability threat. Some researchers suggest that the numerous past reports describing the need to improve cybersecurity have not been compelling enough to make the case for dramatic and urgent action by decision-makers. Others suggest that even though relevant information is available, future possibilities are still discounted, which reduces the apparent need for present-day action. In addition, the costs of current inaction are not borne by the current decision-makers. These researchers argue that IT vendors must be willing to regard security as a product attribute that is coequal with performance and cost; IT researchers must be willing to value cybersecurity research as much as they value research for high performance or cost-effective computing; and, finally, IT purchasers must be willing to incur present-day costs in order to obtain future benefits.[69]

New U.S.A.F. Cyber Command

The Air Force is not laying claim to the cyber domain, but their new mission statement issued in August 2008 indicates they are building a force to operate in that domain. Former Secretary of the Air Force Michael W. Wynne recently stated that the new mission of the U.S. Air Force is to "fly and fight in air, space, and cyberspace." For the Air Force, this means that military action in cyberspace now includes defending against malicious activity on the Internet, and anywhere across the entire electromagnetic spectrum (including the energy spectrum bands for radio, microwaves, infrared, X-ray, and all other options for directed energy), where national security is threatened.[70] Secretary Wynne stated that cyberwarfare flows naturally from the Air Force's traditional missions, such as downloading data from platforms in space, and that U.S. capabilities should be expanded to also enable the shut down of enemy electronic networks.

Air Force officials, led by the Air Force Chief of Staff Gen. Michael Mosley, met at the Pentagon in a "cyberwarfare-themed summit" during November 2006, to make plans for a new Air Force Cyber Command.[71] General Elder stated that the planning session would include an assessment of cyberwarfare requirements to defend the nation.[72]

---

[68] GAO -08-119T, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, October 17, 2007.

[69] Seymour Goodman and Herber Lin, editors, Toward a Safer and More Secure Cyberspace, *Committee on Improving Cybersecurity Research in the United States, National Research Council*, 2007, pp. 261-267, http://books.nap.edu/openbook.php?isbn=0309103959.

[70] John Bennett and Carlo Munoz, *USAF Sets Up First Cyberspace Command*, Military.com, November 4, 2006, http://www.military.com/features/0,15240,118354,00.html.

[71] Contact for Dr. Lani Kass, Director of Air Force Cyberspace Task Force, and Special Assistant to General Michael Moseley, is through Maj. Gary Conn.

[72] Personal communication with Air Force Public Affairs Office, January 26, 2007.

Homeland security reportedly would also be a large part of the Cyber Command's new responsibility, including protection of telecommunications systems, utilities, and transportation. Several issues to be considered may include (1) what kind of educational skills, technical skills, and training are needed for staff at the Cyber Command and (2), what kind of career path can be offered to those in the Air Force who want to participate in defending the new cyber domain.

A provisional team led by AFCYBER Commander Maj. Gen. William T. Lord was starting to look at these issues. Then, Air Force Chief of Staff, Gen. Norton Schwartz, announced October 8, 2008, that there would no longer be a new major command developed for cyberspace operations. Instead the Air Force would continue with standing up a component-Numbered Air Force, which will focus on cyberspace warfighting operations. The 24th Air Force will be led by a 2-star general, and will operate in support of NORTHCOM and STRATCOM missions, which could include anything from hurricane relief to homeland defense. All other administrative, policy and organize-train-equip oversight now falls under Air Force Space Command.

The AFCYBER (P) team will stay formed so they can assist in developing a roadmap to outline the actions needed to transition the work done this past year over to the space command. The provisional team will also assist with other tasks as needed until the new organizational construct is formalized. The new organization will operate on an equal footing with other Numbered Air Force headquarters.

Eventually, there may be a new major command for cyberspace that will stand alongside the Air Force Space Command and the Air Combat Command. Some speculate that there may be a stand-alone combatant command for cyberspace.[73] Precise future command relationships are still being decided in the ongoing planning effort, and more details will be forthcoming.[74]

Joint Command Structure for Cyberwarfare

Currently, the U.S. Strategic Command (USSTRATCOM), which is a unified combatant command for U.S. strategic forces, controls military information operations, space command, strategic warning and intelligence assessments, global strategic operations planning under the Unified Command Plan, and also has overall responsibility for Computer Network Operations (CNO).[75] USSTRATCOM gives most of the daily defense and operational activity to the National Security Agency.

Beneath USSTRATCOM are several Joint Functional Component Commands (JFCCs): (1) space and global strike integration; (2) intelligence, surveillance and reconnaissance; (3) network warfare; (4) integrated missile defense; and (5) combating weapons of mass destruction.[76]

The JFCC-Network Warfare (JFCC-NW), and the JFCC-Space & Global Strike (JFCC-SGS) have responsibility for overall DOD cyber security, while the Joint Task Force-Global Network Operations (JTF-GNO) and the Joint information Operations Warfare Center (JIOWC) both have direct responsibility for defense against cyber attack.[77] The JTF-GNO defends the DOD Global

[73] "New Cyber CoCom Likely" by Colin Clark, DoD Buzz Online Defense and Acquisition Journal, March 6th, 2009 accessed at http://www.dodbuzz.com/2009/03/06/new-cyber-cocom-likely/

[74] Personal communication with Air Force Public Affairs Office, January 26, 2007.

[75] The Public Affairs Office for the Air Force at the Pentagon can be contacted by congressional clients.

[76] United State Strategic Command, July 2006, http://www.stratcom.mil/organization-fnc_comp.html.

[77] Clark A. Murdock et al., Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era, Phase 2 Report, July 2005, Center for Strategic and International Studies, p. 128, http://www.ndu.edu/lIbrary/docs/BeyondGoldwaterNicholsPhase2Report.pdf.

Information Grid, while the JIOWC assists combatant commands with an integrated approach to information operations. These include operations security, psychological operations, military deception, and electronic warfare. The JIOWC also coordinates network operations and network warfare with the JTF-GNO and with JFCC-NW.

Cyberwarrior Education

The President's Comprehensive National Cyber-security Initiative has identified cyber education and training as one of its critical areas of focus. As more U.S. military systems become computerized and linked to networks, some argue there is a growing need for qualified Electronic Warfare operators.[78] In a recent speech, Deputy Secretary of Defense Gordan England said that "in the U.S., the number of scientists and engineers is declining at a time when numbers in many other countries are increasing. This decline in science and technology poses the greatest long-term threat to our country ... including our cyber networks."

Each year, DOD conducts a Cyber Defense Exercise, where teams of students from the nation's military academies advance their cyber skills in practice competition where they deliberately hack into test networks, and also protect these test networks against intrusions by other teams. The Officer Professional Military Education Policy (OPMEP) offers guidance on information operations (IO) and areas related to both IO and command and control (C2), and efforts are underway towards integrating cyber warfare into Joint Professional Military Education curriculum. An impediment to the program is the heavily classified nature of cyberspace doctrine and the international students who comprise some of the student body at the schools.

However, DOD has stated a need to attract, train, and retain skilled information technology professionals beyond those enrolled in the military academies. In an attempt to solve this problem, the Air Force Research Laboratory (AFRL) Cyber Operations Branch offers a 10-week summer program each year for university students, consisting of intensive studies in cyber security. The Advanced Course in Engineering (ACE) Cyber Security Boot Camp has been held at Rome, NY, for the past four years, and involves between 40 and 60 student applicants from Air Force and Army pre-commissioning programs, some National Science Foundation Cyber Corps Fellows, and some civilian college students. For 2006, the theme was "Cybercraft," described as a non-kinetic weapon platform that seeks dominance in cyberspace, corresponding to the new mission of the Air Force to "fly and fight in air, space, and cyberspace," according to program director Dr. Kamal Jabbour. Students study legal and policy issues, cryptography, computer network defense and attack, steganography, and analysis of malicious code. ACE students also spend an average of three days per week in internships at the Air Force Research Laboratory, or with local industry partners, and participate in officer development activities. The faculty for ACE is drawn from Syracuse University, West Point, and Norwich University.

DHS and the National Science Foundation (NSF) have recognized the ACE program as an official internship program for Federal Cyber Service Scholarship for Service (SFS) program. The SFS program seeks to increase the number of skilled students entering the fields of information assurance and cyber security by funding universities to award two-year scholarships in cyber security. Graduates are then required to work for a federal agency for two years. Recent ACE graduates are now working at the Air Force Office of Special Investigations, the AFRL, and the NSA.

Also, as a result of ACE summer program success with college students, in September 2006, Syracuse University developed a special cyber security course to be offered in 12 high schools in

[78] Patience Wait, *Army Shores up EM spectrum skills*, Government Computer News, March 19, 2007.

New Your State. Currently, Syracuse University offers 29 introductory cyber security courses in 148 high schools throughout New York, New Jersey, Maine, Massachusetts, and Michigan. High school students who successfully complete the cyber security courses can receive Syracuse college credits in computer science and engineering.

DOD and the U.S. Critical Infrastructure

DOD officials have noted that because 80% of U.S. commerce goes through the Internet, DOD systems must develop a capability to adequately protect it.[79] Currently, to assist commercially owned telecommunications networks, communications satellite systems, and other civilian critical infrastructure systems, DOD contracts with Carnegie Mellon's Software Engineering Institute to operate the Computer Emergency Response Team (CERT-CC), while DHS, in partnership with private industry, operates a parallel organization called US-CERT. Both organizations monitor trends in malicious code and cyber crime, send out alerts about threats to computer systems, and provide guidance for recovery after an attack.

The Defense Information Systems Agency oversees the military's Global Information Grid (GiG), and provides support for net-centric operations through the JTF-GNO. The GiG is an interconnected set of capabilities that includes any DoD system, equipment, software, or service that transmits, stores, or processes DoD information. The Joint Staff J-6 is working on an initiative called "GiG 2.0," which may take advantage of cloud computing applications and social networking tools. Few details are known about the program at this point, but briefings suggest that the goal is to reconcile the inconsistent security postures and interoperability problems among the multiple service infrastructures by creating a joint DOD enterprise.[80]

Federal Efforts to Protect Computers

The federal government has taken steps to improve its own computer security and to encourage the private sector to also adopt stronger computer security policies and practices to reduce infrastructure vulnerabilities. In 2002, the Federal Information Security Management Act (FISMA) was enacted, giving the Office of Management and Budget (OMB) responsibility for coordinating information security standards and guidelines developed by federal agencies.[81] In 2003, the National Strategy to Secure Cyberspace was published by the Bush Administration to encourage the private sector to improve computer security for the U.S. critical infrastructure through having federal agencies set an example for best security practices.[82]

The OMB has mandated that all U.S. Government enable their networks to handle traffic from IPv6, a next generation set of internet protocols. IPv6 was developed in response to the imminent exhaustion of IP addresses; the new system will allow more flexibility in address assignment, and simplifies the translating mechanism used to route traffic to particular sites. Network security is

[79] John Doyle, *Air Force To Elevate Status Of Cyberspace Command,* Aerospace Daily & Defense Report, March 22, 2007.

[80] Vice Admiral Nancy Brown, Director for Command, Control, Communications and Computer Systems, *GIG 2.0*, (J-6) The Joint Staff, Presentation at AFCEA Solution Series: Information Assurance, Washington, DC, September 9, 2008, http://www.afcea.org/events/solutions/08/infoassurance/files/Tue_1300_Brown.pdf.

[81] GAO has noted that many federal agencies have not implemented security requirements for most of their systems, and must meet new requirements under FISMA. See GAO Report GAO-03-852T, *Information Security: Continued Efforts Needed to Fully Implement Statutory Requirements*, June 24, 2003.

[82] Tinabeth Burton, *ITAA Finds Much to Praise in National Cybersecurity Plan*, May 7, 2003, http://www.findarticles.com/p/articles/mi_go1965/is_200303/ai_n7418485.

also a built-in feature of IPv6 architecture, and government systems running it are anticipated to be more secure. Federal agencies now support the IPv6 protocol and its interoperability, but are not necessarily using it on a day-to-day basis. Full operational transition to IPv6 remains a future goal.

The National Cyber Security Division (NCSD), within the National Protection and Programs Directorate of the Department of Homeland Security (DHS) oversees a Cyber Security Tracking, Analysis and Response Center (CSTARC), tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and warnings for cyberthreats, improving information sharing, responding to major cybersecurity incidents, and aiding in national-level recovery efforts. In addition, a new Cyber Warning and Information Network (CWIN) has begun operation in 50 locations, and serves as an early warning system for cyberattacks.[83] The CWIN is engineered to be reliable and survivable, has no dependency on the Internet or the public switched network (PSN), and reportedly will not be affected if either the Internet or PSN suffer disruptions.[84]

In January 2004, the NCSD also created the National Cyber Alert System (NCAS), a coordinated national cybersecurity system that distributes information to subscribers to help identify, analyze, and prioritize emerging vulnerabilities and cyberthreats. NCAS is managed by the United States Computer Emergency Readiness Team (US-CERT), a partnership between NCSD and the private sector, and subscribers can sign up to receive notices from this new service by visiting the US-CERT website.[85]

To observers, the most pervasive question regarding cyberattack and response is, "Who's in charge?" In an attempt to clarify roles and responsibilities and to develop an all-encompassing strategy, then president George W. Bush launched a $30 billion dollar Comprehensive National Cybersecurity Initiative (CNCI) in 2008 to prioritize and coordinate cyber defense across government. The initiative was prompted by the Director of National Intelligence's urging, and was led by ODNI's Joint Interagency Cyber Task Force. The Obama administration is continuing this effort by conducting a 60-day cybersecurity review, led by Melissa Hathaway, who was the coordinator of the ODNI task force. (For more on the CNCI, see CRS Report R40427, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John Rollins and Anna C. Henning.)

DHS is lead agency for the Federal Government's cybersecurity; it coordinates government and private-sector efforts through its National Cyber Security Center (NCSC). However, there are high-ranking officials who assert that NSA should run the government's cybersecurity efforts as it does for the military. The resident technological talent within NSA and the benefits of having both defensive and offensive capabilities co-located make the idea attractive to some. Critics point towards allegations of NSA's civil liberties violations with internet monitoring programs, and say that having this one agency in charge of all things cyber will erode the public trust. Also, the private sector may be less inclined to work cooperatively with the NSA—which they maintain would present a big problem, as 80% of the United States infrastructure is privately owned. There have also been criticisms that DHS's cyber programs are inadequately funded, and that the leadership lacks the authority necessary to push forward its initiatives. To illustrate this point,

[83] Bara Vaida, "Warning Center for Cyber Attacks is Online, Official Says," *Daily Briefing*, GovExec.com, June 25, 2003.

[84] The Cyber Warning Information Network (CWIN) provides voice and data connectivity to government and industry participants in support of critical infrastructure protection, http://www.publicsectorinstitute.net/ELetters/HomelandSecurityStrategies/Volume1No1/CyberWarningNetLaunch.lsp.

[85] http://www.us-cert.gov/cas/.

Rob Beckstrom, the director of the NCSC resigned on March 6, 2009 over concerns that the NSA was "dominating" cybersecurity efforts. At a hearing on March 10, 2009, several experts testifying before the House Subcommittee on Emerging Threats, Cybersecurity and Science and Technology echoed this sentiment.[86] (For a thorough discussion of reforming the national security structure to meet today's challenges, see CRS Report RL34455, *Organizing the U.S. Government for National Security: Overview of the Interagency Reform Debates*, by Catherine Dale, Nina M. Serafino, and Pat Towell.)

Policy Issues

Several areas for possible congressional consideration are:

- help to determine appropriate responses by DOD to a cyberattack;
- examine the incentives for achieving the goals of the National Strategy to Secure Cyberspace and the CNCI, or for developing a new national strategy;
- search for ways to improve the security of commercial software products;
- explore ways to increase security education and awareness for businesses and home PC users; and
- find ways for private industry and government to coordinate to protect against cyberattack.
- reconsider classification levels to allow for increased information sharing
- oversight for DOD execution of cyberdefense appropriations

Congress may also wish to consider ways to harmonize existing federal and state laws that require notice to persons when their personal information has been affected by a computer security breach, and that impose obligations on businesses and owners of that restricted information.[87]

DOD and Cyberattack Response

If a terrorist group were to use a cybercrime botnet to subvert computers in a third party country, such as China, to launch a cyberattack against the United States, the U.S. response to the cyberattack would presumably need to be carefully considered, in order to avoid retaliating against the wrong entity. Would the resulting effects of cyberweapons used by the United States be difficult to limit or control? Would a cyberattack response that could be attributed to the United States possibly encourage other extremists, or rogue nations, to start launching their own cyberattacks against the United States? Would an attempt by the U.S. to increase surveillance of another entity via use of cyberespionage computer code be labeled as an unprovoked attack, even if directed against the computers belonging to a terrorist group? If a terrorist group should subsequently copy, or reverse-engineer a destructive U.S. military cyberattack program, could it be used against other countries that are U.S. allies, or even turned back to attack civilian computer systems in the United States?[88] If the effects become widespread and severe, could the

[86] This testimony can be accessed at http://homeland.house.gov/hearings/index.asp?ID=175

[87] For more information about laws related to identity theft, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Marie Stevens.

[88] See CRS Report RL31787, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson.

U.S. use of cyberweapons exceed the customary rules of military conflict, or violate international laws?[89]

Commercial electronics and communications equipment are now used extensively to support complex U.S. weapons systems, and are possibly vulnerable to cyberattack. This situation is known to our potential adversaries.[90] To what degree are military forces and national security threatened by computer security vulnerabilities that exist in commercial software systems, and how can the computer industry be encouraged to create new commercial off-the-shelf (COTS) products that are less vulnerable to cyberattack?

Incentives for the National Strategy to Secure Cyberspace

Does the National Strategy to Secure Cyberspace present clear incentives for achieving security objectives? Suggestions to increase incentives may include requiring that all software procured for federal agencies be certified under the "Common Criteria" testing program, which is now the requirement for the procurement of military software. However, industry observers point out that the software certification process is lengthy and may interfere with innovation and competitiveness in the global software market.[91]

Should the National Strategy to Secure Cyberspace rely on voluntary action on the part of private firms, home users, universities, and government agencies to keep their networks secure, or is there a need for possible regulation to ensure best security practices? Has public response to improve computer security been slow partly because there are no regulations currently imposed?[92] Would regulation to improve computer security interfere with innovation and possibly harm U.S. competitiveness in technology markets? Two of the former cybersecurity advisers to the president have differing views: Howard Schmidt has stated that market forces, rather than the

[89] The laws of war are international rules that have evolved to resolve practical problems relating to military conflict, such as restraints to prevent misbehavior or atrocities, and have not been legislated by an overarching central authority. The United States is party to various limiting treaties. Sometimes the introduction of new technology tends to force changes in the understanding of the laws of war. Gary Anderson and Adam Gifford, "Order Out of Anarchy: The International Law of War," *The Cato Journal*, August 2004, vol. 15, no. 1, pp. 25-36.

[90] Stanley Jakubiak and Lowell Wood, "DOD Uses Commercial Software and Equipment in Tactical Weapons," Statements before the House Military Research and Development Subcommittee, Hearing on EMP Threats to the U.S. Military and Civilian Infrastructure, October 7, 1999. House Armed Services Committee, *Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*, hearing, July 22, 2004.

[91] Agencies operating national security systems are required to purchase software products from a list of lab-tested and evaluated products in a program run by the National Information Assurance Partnership (NIAP), a joint partnership between the National Security Agency and the National Institute of Standards and Technology. The NIAP is the U.S. government program that works with organizations in a dozen other countries around the world which have endorsed the international security-evaluation regimen known as the "Common Criteria." The program requires vendors to submit software for review in an accredited lab, a process that often takes a year and costs several thousand dollars. The review previously was limited to military national security software and equipment, however, the Administration has stated that the government will undertake a review of the program to "possibly extend" this software certification requirement to civilian agencies. Ellen Messmer, White House issue "National Strategy to Secure Cyberspace," *Network World Fusion*, February 14, 2003, at http://www.nwfusion.com/news/2003/0214ntlstrategy.html.

[92] Business executives may be cautious about spending for large new technology projects, such as placing new emphasis on computer security. Results from a February 2003 survey of business executives indicated that 45% of respondents believed that many large Information Technology (IT) projects are often too expensive to justify. Managers in the survey pointed to the estimated $125.9 billion spent on IT projects between 1977 and 2000 in preparation for the year 2000 (Y2K) changeover, now viewed by some as a non-event. Sources reported that some board-level executives stated that the Y2K problem was overblown and over funded then, and as a result, they are now much more cautious about future spending for any new, massive IT initiatives. Gary H. Anthes and Thomas Hoffman, "Tarnished Image," *Computerworld*, May 12, 2003, vol. 37, no. 19, p. 37.

government, should determine how product technology should evolve for better cybersecurity; however, Richard Clarke has stated that the IT industry has done little on its own to improve security of its own systems and products.[93]

Improving Security of Commercial Software

Some security experts emphasize that if systems administrators received the necessary training for keeping their computer configurations secure, then computer security would greatly improve for the U.S. critical infrastructure. However, should software product vendors be required to create higher quality software products that are more secure and that need fewer patches? Could software vendors possibly increase the level of security for their products by rethinking the design, or by adding more test procedures during product development?

Education and Awareness of Cyberthreats

Ultimately, many observers argue that reducing the threat to national security from cybercrime depends on a strong commitment by government and the private sector to follow best management practices that help improve computer security. Numerous government reports already exist that describe the threat of cybercrime and make recommendations for management practices to improve cybersecurity.

A 2004 survey done by the National Cyber Security Alliance and AOL showed that most home PC users do not have adequate protection against hackers, do not have updated antivirus software protection, and are confused about the protections they are supposed to use and how to use them.[94] How can computer security training be made available to all computer users that will keep them aware of constantly changing computer security threats, and that will encourage them to follow proper security procedures?

Coordination Between Private Sector and Government

What can be done to improve sharing of information between federal government, local governments, and the private sector to improve computer security? Effective cybersecurity requires sharing of relevant information about threats, vulnerabilities, and exploits.[95] How can the private sector obtain information from the government on specific threats which the government now considers classified, but which may help the private sector protect against cyberattack? How can the government obtain specific information from private industry about the number of successful computer intrusions, when companies resist reporting because they want to avoid

[93] Howard Schmidt points out that major technology firms now promote anti-virus software and encourage better cybersecurity practices. He stresses that market forces are causing private industry to improve security of products. Martin Kady, "Cybersecurity a Weak Link in Homeland's Armor," *CQ Weekly*, February 14, 2005. Meanwhile, Richard Clarke, who initially opposed regulation during his tenure in the Clinton and Bush administrations, now states that the IT industry only responds to improve security of its products when regulation is threatened. William Jackson, "To Regulate or Not to Regulate? That Is the Question," *Government Computer New*s, February 26, 2005.

[94] A 2004 survey of 329 PC users revealed that most computer users think they are safe but lack basic protections against viruses, spyware, hackers, and other online threats. In addition, large majorities of home computer users have been infected with viruses and spyware and remain highly vulnerable to future infections. AOL and the National Cyber Security Alliance, "Largest In-home Study of Home Computer Users Shows Major Online Threats, Perception Gap," October 2004 at http://www.staysafeonline.info/news/NCSA-AOLIn-HomeStudyRelease.pdf.

[95] Government Accountability Office, *Homeland Security: Efforts To Improve Information Sharing Need to Be Strengthened*, GAO-03-760, August 2003.

publicity and guard their trade secrets?[96] Should cybercrime information voluntarily shared with the federal government about successful intrusions be shielded from disclosure through Freedom of Information Act requests?

How can the United States better coordinate security policies and international law to gain the cooperation of other nations to better protect against a cyberattack? Pursuit of hackers may involve a trace back through networks requiring the cooperation of many Internet Service Providers located in several different nations.[97] Pursuit is made increasingly complex if one or more of the nations involved has a legal policy or political ideology that conflicts with that of the United States.[98]

Thirty-eight countries, including the United States, participate in the Council of Europe's Convention on Cybercrime, which seeks to combat cybercrime by harmonizing national laws, improving investigative abilities, and boosting international cooperation. However, how effective will the Convention without participation of other countries where cybercriminals now operate freely? (For more on the Convention, see CRS Report RS21208, *Cybercrime: The Council of Europe Convention*, by Kristin Archick.)

Legislative Activity in the 110th Congress

H.R. 1525—The Internet Spyware (I-SPY) Prevention Act of 2007, proposed penalties for unauthorized access to computers, or the use of computers to commit crimes. The bill passed the House on May 22, 2007. On May 23, 2007, this bill was received in the Senate and referred to the Committee on the Judiciary.

H.R. 1684—The Department of Homeland Security Authorization Act for Fiscal Year 2008 established within the Department of Homeland Security an Office of Cybersecurity and Communications, headed by the Assistant Secretary for Cybersecurity and Communications, with responsibility for overseeing preparation, response, and reconstitution for cybersecurity and to protect communications from terrorist attacks, major disasters, and other emergencies, including large-scale disruptions.

The bill directed the Assistant Secretary to do the following:

- Establish and maintain a capability within the Department for ongoing activities to identify threats to critical information infrastructure to aid in detection of vulnerabilities and warning of potential acts of terrorism and other attacks.
- Conduct risk assessments on critical information infrastructure with respect to acts of terrorism.
- Develop a plan for the continuation of critical information operations in the event of a cyber attack.
- Define what qualifies as a cyber incident of national significance for purposes of the National Response Plan.

[96] CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

[97] Trace back to identify a cyberattacker at the granular level remains problematic. Dorothy Denning, *Information Warfare and Security* (Addison-Wesley, 1999), p. 217.

[98] In Argentina, a group calling themselves the X-Team, hacked into the website of that country's Supreme Court in April 2002. The trial judge stated that the law in his country covers crime against people, things, and animals but not websites. The group on trial was declared not guilty of breaking into the website. Paul Hillbeck, "Argentine Judge Rules in Favor of Computer Hackers," February 5, 2002, at http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3070194.htm.

- Develop a national cybersecurity awareness, training, and education program that promotes cybersecurity awareness within the Federal Government and throughout the Nation.
- Consult and coordinate with the Under Secretary for Science and Technology on cybersecurity research and development to strengthen critical information infrastructure against acts of terrorism.

This bill passed the House on May 9, 2007. On May 11, 2007, this bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

H.R. 3237—The Smart Grid Facilitation Act of 2007 proposed to modernize the Nation's electricity transmission and distribution system to incorporate digital information and controls technology. "Smart grid" technology functions would include the ability to detect, prevent, respond to, or recover from cyber-security threats and terrorism. The new Grid Modernization Commission would be directed to undertake, and update on a biannual basis, an assessment of the progress toward modernizing the electric system including cybersecurity protection for extended grid systems. On August 24, 2007, the bill was referred to House subcommittee on Energy and Environment.

H.R. 3221—The New Direction for Energy Independence, National Security, and Consumer Protection Act proposed establishment of the Grid Modernization Commission to facilitate the adoption of Smart Grid standards, technologies, and practices across the Nation's electricity grid. This bill became P.L. 110-289 on July 30, 2008.

H.R. 1585, the National Defense Authorization Act for Fiscal Year 2008, required the Secretary of Defense to conduct a quadrennial roles and missions review for the Department of Defense, which will also include cyber operations. This bill became P.L. 110-181 on January 28, 2008.[99]

H.Rept. 110-146, on H.R. 1585, by the Committee on Armed Services. This report stated that within 180 days after enactment of the National Defense Authorization Act for 2008, the Secretary of Defense must submit a report to congressional defense committees, with the following requirements:

1. Review legal authorities to ensure effective cyberspace operations.

2. Review DOD's policies for information sharing and risk management for cyberspace operations.

3. Provide an overview of DOD's cyberspace organization, strategy, and programs.

4. Assess operational challenges, including the impact of the military's reliance on commercial communications infrastructure.

5. Recommend ways to improve DOD's ability to coordinate cyberspace operations with law enforcement, intelligence communities, the commercial sector, and with international allies. The recommendations shall include consideration of the establishment of a single joint organization for cyberspace operations.

6. Provide an overview of training and educational requirements.

7. Provide an overview of funding for cyberspace operations.

[99] Department of Defense, *Quadrennial Roles and Missions Review Report*, January 2009, pg. 14.

The DOD Roles and Missions Review report, issued in January 2009, placed cyberspace high on the list of focus areas, and asserted that this domain will be one in which major combat operations may take place.

Potential Future Issues for Congress

Could provocative actions, for example, intelligence gathering by the U.S. military that involves using intrusive cyber or electronic warfare tools to monitor enemy system activity, or copy important data files, be challenged by other nations as a violation of the law of Armed Conflict? Exploratory intrusions by U.S. military computers to gather intelligence may provoke other strong or unexpected responses from some countries or extremist groups that are targeted for monitoring by DOD.

Several questions also may arise when considering a retaliatory cyber or electronic warfare counterstrike: (1) if the attacker is a civilian, should the attack be considered a law enforcement problem rather than a military matter?; (2) if a U.S. military cyberattack against a foreign government also disables civilian infrastructure, can it be legally justified?; or (3) how can the military be certain that a targeted foreign computer system has not been innocently set up to appear as an attacker by another third party attacker?

Some observers have stated that success in future conflicts will depend less on the will of governments, and more on the perceptions of populations, and that perception control will be achieved and opinions shaped by the warring group that best exploits the global media.[100] As a result of the increasingly sophisticated use of networks by terrorist groups and the potentially strong influence of messages carried by the global media, does DOD now view the Internet and the mainstream media as a possible threat to the success of U.S. military missions? How strongly will U.S. military PSYOP be used to manipulate public opinion, or reduce opposition to unpopular decisions in the future?

Another emerging issue may be whether DOD is legislatively authorized to engage in PSYOP that may also affect domestic audiences.[101] DOD Joint Publication 3-13, released February 2006, provides current doctrine for U.S. military Information Operations, and explains the importance of achieving information superiority.[102] However, the DOD Information Operations Roadmap, published October 2003, states that PSYOP messages intended for foreign audiences increasingly are consumed by the U.S. domestic audience, usually because they can be re-broadcast through the global media. The Roadmap document states that, " ... the distinction between foreign and domestic audiences becomes more a question of USG (U.S. Government) intent rather than information dissemination practices (by DOD)."[103] This may be interpreted to mean that DOD has no control over who consumes PSYOP messages once they are re-transmitted by commercial media.

[100] Maj. Gen. Robert Scales (Ret), *Clausewitz and World War IV*, Armed Forces Journal, July 2006, p. 19.

[101] Psychological Operations are authorized for the military under Title 10, USC, Subtitle A, Part I, Chapter 6, Section 167, "Unified Combatant Command for Special Operations Forces."

[102] DOD Joint Publication 3-13, Information Operations, February 13, 2006, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

[103] DOD Information Operations Roadmap, October 30, 2003, p. 26. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

Appendix A. Definitions

Information

Information is a resource created from two things: phenomena (data) that are observed, plus the instructions (systems) required to analyze and interpret the data to give it meaning. The value of information is enhanced by technology, such as networks and computer databases, which enables the military to (1) create a higher level of shared awareness, (2) better synchronize command, control, and intelligence, and (3) translate information superiority into combat power.

DOD Information Operations

The current DOD term for military information warfare is "Information Operations" (IO). DOD information operations are actions taken during time of crisis or conflict to affect adversary information, while defending one's own information systems, to achieve or promote specific objectives.[104] The focus of IO is on disrupting or influencing an adversary's decision-making processes.

An IO attack may take many forms, for example: (1) to slow adversary computers, the software may be disrupted by transmitting a virus or other malicious code; (2) to disable sophisticated adversary weapons, the computer circuitry may be overheated with directed high energy pulses; and (3) to misdirect enemy sensors, powerful signals may be broadcast to create false images. Other methods for IO attack may include psychological operations such as initiating TV and radio broadcasts to influence the opinions and actions of a target audience, or seizing control of network communications to disrupt an adversary's unity of command.

Computer Network Defense (CND) is the term used to describe activities that are designed to protect U.S. forces against IO attack from adversaries. Part of CND is information assurance (IA), which requires close attention to procedures for what is traditionally called computer and information security.

DOD places new emphasis on the importance of dominating the entire electromagnetic spectrum with methods for computer network attack and electronic warfare. DOD also emphasizes that because networks are increasingly the operational center of gravity for warfighting, the U.S. military must be prepared to "fight the net."[105] Because the recently declassified source document containing this phrase has some lines blacked out, it is not clear if "... net" means the Internet. If so, then this phrase may be a recognition by DOD that Psychological Operations, including public affairs work and public diplomacy, must be employed in new ways to counter the skillful use of the Internet, social networking tools, and the global news media by U.S. adversaries.

[104] From the *DOD Dictionary of Military and Associated Terms*, January 2003, http://www.dtic.mil/doctrine/jel/doddict/data/i/index.html.

[105] DOD Information Operations Roadmap, October 30, 2003, p. 6-7, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

Appendix B. DOD Information Operations Core Capabilities

In Joint Publication 3-13, DOD identifies five core capabilities, or "pillars," for conduct of information operations: (1) Psychological Operations, (2) Military Deception, (3) Operations Security, (4) Computer Network Operations, and (5) Electronic Warfare.[106] These capabilities are interdependent, and increasingly are integrated to achieve desired effects.

Psychological Operations (PSYOP)

DOD defines PSYOP as planned operations to convey selected information to targeted foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[107] For example, during the Operation Iraqi Freedom (OIF), broadcast messages were sent from Air Force EC-130E aircraft, and from Navy ships operating in the Persian Gulf, along with a barrage of e-mail, faxes, and cell phone calls to numerous Iraqi leaders encouraging them to abandon support for Saddam Hussein.

The civilian Al Jazeera news network, based in Qatar, beams its messages to well over 35 million viewers in the Middle East, and is considered by many to be a "market competitor" for U.S. PSYOP. Terrorist groups can also use the Internet to quickly place their own messages before an international audience. Some observers have stated that the U.S. will continue to lose ground in the global media wars until it develops a coordinated strategic communications strategy to counter competitive civilian news media, such as Al Jazeera.[108]

Partly in response to this observation, DOD now emphasizes that PSYOP must be improved and focused against potential adversary decision making, sometimes well in advance of times of conflict. Products created for PSYOP must be based on in-depth knowledge of the audience's decision-making processes. Using this knowledge, the PSYOPS products then must be produced rapidly, and disseminated directly to targeted audiences throughout the area of operations.[109]

Following the Smith-Mundt Act, DOD policy prohibits the use of PSYOP for targeting American audiences.[110] However, while military PSYOP products are intended for foreign targeted audiences, DOD also acknowledges that the global media may pick up some of these targeted messages, and replay them back to the U.S. domestic audience. Therefore, a sharp distinction between foreign and domestic audiences cannot be maintained.[111]

Military Deception (MILDEC)

Deception guides an enemy into making mistakes by presenting false information, images, or statements. MILDEC is defined as actions executed to deliberately mislead adversary military decision makers with regard to friendly military capabilities, thereby causing the adversary to

[106] JP 3-13 Information Operations, February 13, 2006.

[107] *DOD Dictionary of Military Terms*, http://www.dtic.mil/doctrine/jel/doddict/.

[108] Air Force, *Operation Iraqi Freedom Information Operations Lessons Learned: First Look*, AFC2ISRC/CX, July 23, 2003, http://www.insidedefense.com/secure/data_extra/pdf3/dplus2004_265.pdf.

[109] DOD Information Operations Roadmap, October 30, 2003, p. 6, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

[110] 22 USC Chapter 18, "The United States Information and Educational Exchange Act of 1948."

[111] DOD Information Operations Roadmap, October 30, 2003, p. 26, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

take (or fail to take) specific actions that will contribute to the success of the friendly military operation.

As an example of deception during Operation Iraqi Freedom (OIF), the U.S. Navy deployed the Tactical Air Launched Decoy system to divert Iraqi air defenses away from real combat aircraft.

Operational Security (OPSEC)

OPSEC is defined as a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities. For example, during OIF, U.S. forces were warned to remove certain information from DOD public websites, so that Iraqi forces could not exploit sensitive but unclassified information.

Computer Network Operations (CNO)

CNO includes the capability to: (1) attack and disrupt enemy computer networks; (2) defend our own military information systems; and (3) exploit enemy computer networks through intelligence collection, usually done through use of computer code and computer applications. The Joint Information Operations Warfare Command (JIOWC) and the Joint Functional Component Command for Network Warfare (JFCCNW) are responsible for the evolving mission of Computer Network Attack.[112] The exact capabilities of the JIOWC and JFCCNW are highly classified, and DOD officials have reportedly never admitted to launching a cyber attack against an enemy, however many computer security officials believe the organization can destroy networks and penetrate enemy computers to steal or manipulate data, and take down enemy command-and-control systems. They also believe that the organization consists of personnel from the CIA, National Security Agency, FBI, the four military branches, and civilians and military representatives from allied nations.[113] The Joint Task Force for Global Network Operations (JTF-GNO), currently residing within the Defense Information Security Agency (DISA), is an operational arm of the services. A recent decision to move the JTF-GNO under the auspices of the National Security Agency will put defensive and operational capabilities within the same organization.[114]

Computer Network Defense (CND)

CND is defined as defensive measures to protect information, computers, and networks from disruption or destruction. CND includes actions taken to monitor, detect, and respond to unauthorized computer activity. Responses to IO attack against U.S. forces may include use of passive information assurance tools, such as firewalls or data encryption, or may include more intrusive actions, such as monitoring adversary computers to determine their capabilities before they can attempt an IO attack against U.S. forces.

Some DOD officials believes that CND may lack sufficient policy and legal analysis for guiding appropriate responses to intrusions or attacks on DOD networks. Therefore, DOD has recommended that a legal review be conducted to determine what level of intrusion or data

[112] John Lasker, *U.S. Military's Elite Hacker Crew*, Wired News, April 18, 2005, http://www.wired.com/news/privacy/0,1848,67223,00.html, U.S. Strategic Command Fact File http://www.stratcom.mil/fact_sheets/fact_jtf_gno.html and http://www.stratcom.mil/fact_sheets/fact_jioc.html.

[113] John Lasker, *U.S. Military's Elite Hacker Crew*, April 18, 2005, Wired News, http://www.wired.com/news/privacy/0,67223-0.html?tw=wn_story_page_prev2.

[114] Some fear this move will have negative repercussions on civil liberties.

manipulation constitutes an attack. The distinction is necessary in order to clarify whether an action should be called an attack or an intelligence collection operation, and which aggressive actions can be appropriately taken in self-defense. This legal review should also determine if appropriate authorities permit U.S. forces to retaliate through manipulation of unwitting third party computer hosts. And finally, DOD has recommended structuring a legal regime that applies separately to domestic and to foreign sources of computer attack against DOD or the U.S. critical. infrastructure.[115]

Computer Network Exploitation (CNE)

CNE is an area of IO that is not yet clearly defined within DOD. Before a crisis develops, DOD seeks to prepare the IO battlespace through intelligence, surveillance, and reconnaissance, and through extensive planning activities. This involves intelligence collection, that in the case of IO, is usually performed through network tools that penetrate adversary systems to gain information about system vulnerabilities, or to make unauthorized copies of important files. Tools used for CNE are similar to those used for computer attack, but configured for intelligence collection rather than system disruption. Although CNE is an activity designed for data exfiltration, it is unknown whether the methods used to penetrate networks could also be used for an attack by an adversary.

Computer Network Attack (CNA)

CNA is defined as effects intended to disrupt or destroy information resident in computers and computer networks. As a distinguishing feature, CNA normally relies on a data stream used as a weapon to execute an attack. For example, sending a digital signal stream through a network to instruct a controller to shut off the power flow is CNA, while sending a high voltage surge through the electrical power cable to short out the power supply is considered Electronic Warfare (However, a digital stream of computer code or a pulse of electromagnetic power can both be used to also create false images in adversary computers).

During Operation Iraqi Freedom, U.S. and coalition forces reportedly did not execute any computer network attacks against Iraqi systems. Even though comprehensive IO plans were prepared in advance, DOD officials stated that top-level approval for several CNA missions was not granted until it was too late to carry them out to achieve war objectives.[116] U.S. officials may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to a financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe as well. Such global network interconnections, plus close network links between Iraqi military computer systems and the civilian infrastructure, reportedly frustrated attempts by U.S. forces to design a cyber attack that would be limited to military targets only in Iraq.[117]

In a meeting held in January 2003, at the Massachusetts Institute of Technology, White House officials sought input from experts outside government on guidelines for use of cyber-warfare.

---

[115] DOD Information Operations Roadmap, October 30, 2003, p. 52. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

[116] Elaine Grossman, "Officials: Space, Info Targets Largely Cobbled On-The-Fly for Iraq," *Inside the Pentagon,* May 29, 2003.

[117] Charles Smith, "U.S. Information Warriors Wrestle with New Weapons," *NewsMax.com,* March 13, 2003 http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml.

Officials have stated they are proceeding cautiously, since a cyberattack could have serious cascading effects, perhaps causing major disruption to networked civilian systems.[118] In February 2003, the Bush Administration announced national-level guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems. The classified guidance, known as National Security Presidential Directive 16, is intended to clarify circumstances under which a disabling computer attack would be justified, and who has authority to launch such an attack.

Electronic Warfare (EW)

EW is defined by DOD as any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring.[119] Directed energy weapons amplify, or disrupt, the power of an electromagnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems. The Electronic Warfare Division of the Army Asymmetric Warfare Office has responsibility for creating electronic warfare policy, and for supporting development of new electromagnetic spectrum concepts that can be translated into equipment and weapons.

Domination of the Electromagnetic Spectrum

DOD now emphasizes maximum control of the entire electromagnetic spectrum, including the capability to disrupt all current and future communication systems, sensors, and weapons systems. This may include (1) navigation warfare, including methods for offensive space operations where global positioning satellites may be disrupted; or, (2) methods to control adversary radio systems; and, (3) methods to place false images onto radar systems, block directed energy weapons, and misdirect unmanned aerial vehicles (UAVs) or robots operated by adversaries.[120]

For example, military IO testing examined the capability to secretly enter an enemy computer network and monitor what their radar systems could detect. Further experiments tested the capability to take over enemy computers and manipulate their radar to show false images.[121]

Electromagnetic Non-Kinetic Weapons

Non-kinetic weapons emit directed electromagnetic energy that, in short pulses, may permanently disable enemy computer circuitry. For example, an electromagnetic non-kinetic weapon mounted in an aircraft, or on the ground, might disable an approaching enemy missile by directing a High Power Microwave (HPM) beam that burns out the circuitry, or that sends a false telemetry signal

[118] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," *Washington Post*, February 7, 2003, Section A, p. 1.

[119] CRS Report RL32544, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*, by Clay Wilson.

[120] DOD Information Operations Roadmap, October 30, 2003, p. 61. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

[121] These programs were called Suter 1 and Suter 2, and were tested during Joint Expeditionary Forces Experiments held at Nellis Air Force Base in 2000 and 2002. David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p. 34.

to misdirect the targeting computer.[122] Also, at reduced power, electromagnetic non-kinetic weapons can also be used as a non-lethal method for crowd control.

The Active Denial System (ADS), developed by the Air Force, is a vehicle-mounted nonlethal, counter-personnel directed energy weapon. Currently, most non-lethal weapons for crowd control, such as bean-bag rounds, utilize kinetic energy. However, the ADS projects a focused beam of millimeter energy waves to induce an intolerable burning sensation on an adversary's skin, repelling the individual without causing injury. Proponents say the ADS is safe and effective at ranges between 50 and 1,600 feet. The nonlethal capabilities of the ADS are designed to protect the innocent, minimize fatalities, and limit collateral damage.[123] Approximately $40 million has been spent on this technology over the past ten years.

Military officials requested that ADS devices be deployed to Iraq to assist Marines in guarding posts, countering insurgent snipers and protecting convoys. In July 2005, it was reported that the Active Denial System would be deployed to Iraq before the end of the year. Under an initiative called Project Sheriff, troops would receive a total of 15 vehicles. Concerns of political fallout have delayed these plans; as of early 2007, initial deployment was slated no sooner than 2010.

The ADS system would be the first operationally deployed directed-energy weapon for counter-personnel missions.[124]

Author Information

Catherine A. Theohary
Analyst in National Security Policy and Information Operations

Disclaimer

[122] David Fulghum, "Sneak Attack," *Aviation Week & Space Technology*, June 28, 2004, p. 34.

[123] Active Denial System, Fact Sheet, Air Force Research Lab, Office of Public Affairs, Kirtland Air Force Base, http://www.de.afrl.af.mil/Factsheets/ActiveDenial.pdf.

[124] Jason Sherman, *Pentagon Considering Sending Non-Lethal Ray Gun to Iraq*, Inside Defense, March 2, 2007.