Congressional Research Service

Report RL32114

Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress

Clay Wilson, Foreign Affairs, Defense, and Trade Division

January 29, 2008

Abstract. This report discusses options now open to nation states, extremists, or terrorist groups for obtaining malicious technical services from cybercriminals to meet political or military objectives, and describes the possible effects of a coordinated cyberattack against the U.S. critical infrastructure.

Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress

Clay Wilson
Specialist in Military Information Technology

January 29, 2008

Congressional Research Service
7-5700
www.crs.gov
RL32114

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Cybercrime is becoming more organized and established as a transnational business. High technology online skills are now available for rent to a variety of customers, possibly including nation states, or individuals and groups that could secretly represent terrorist groups. The increased use of automated attack tools by cybercriminals has overwhelmed some current methodologies used for tracking Internet cyberattacks, and vulnerabilities of the U.S. critical infrastructure, which are acknowledged openly in publications, could possibly attract cyberattacks to extort money, or damage the U.S. economy to affect national security.

In April and May 2007, NATO and the United States sent computer security experts to Estonia to help that nation recover from cyberattacks directed against government computer systems, and to analyze the methods used and determine the source of the attacks. (See Larry Greenemeier, "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter,'" *Information Week*, May 24, 2007, at http://www.informationweek.com/news/showArticle.jhtml?articleID=199701774.) Some security experts suspect that political protestors may have rented the services of cybercriminals, possibly a large network of infected PCs, called a "botnet," to help disrupt the computer systems of the Estonian government. DOD officials have also indicated that similar cyberattacks from individuals and countries targeting economic, political, and military organizations may increase in the future. (See 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. and Sebastian Sprenger, "Maj. Gen. Lord Is a Groundbreaker," *Federal Computer Week*, October 15, 2007, vol. 21, no. 34, p. 44.)

Cybercriminals have reportedly made alliances with drug traffickers in Afghanistan, the Middle East, and elsewhere where profitable illegal activities are used to support terrorist groups. In addition, designs for cybercrime botnets are becoming more sophisticated, and future botnet architectures may be more resistant to computer security countermeasures. (See Tom Espiner, "Security Expert: Storm Botnet 'Services' Could Be Sold," CnetNews.com, October 16, 2007, http://www.news.com/Security-expert-Storm-botnet-services-could-be-sold/2100-7349_3-6213781.html.)

This report discusses options now open to nation states, extremists, or terrorist groups for obtaining malicious technical services from cybercriminals to meet political or military objectives, and describes the possible effects of a coordinated cyberattack against the U.S. critical infrastructure. This report will be updated as events warrant.

Contents

Figures

Contacts

Introduction

The U.S. military is supported partly by civilian high technology services and products, most often in the form of communications systems and computer software.[1] In future conflicts that involve cyberwarfare between nations, the distinction between U.S. military and civilian targets may be blurred and civilian computer systems may increasingly be seen as viable targets vulnerable to attack by adversaries.[2]

Computer networking technology has also blurred the boundaries between cyberwarfare, cybercrime, and cyberterrorism. Officials in government and industry now say that cybercrime and cyberattack services available for hire from criminal organizations are a growing threat to national security as well as to the U.S. economy.[3] New and sophisticated cybercrime tools could operate to allow a nation state or terrorist group to remain unidentified while they direct cyberattacks through the Internet.[4] Many experts point out that past incidents of conventional terrorism have already been linked with cybercrime, and that computer vulnerabilities may make government and civilian critical infrastructure systems seem attractive as targets for cyberattack.[5] Some experts argue that the government of Estonia may have already experienced this type of cyberattack directed against their systems and websites in April, 2007.

This report explores the possible connections between cybercriminals and terrorist groups that want to damage the U.S. economy or national security interests. The report also examines the effects of a coordinated cyberattack against the U.S. critical infrastructure, including use of cybercrime tools that could possibly take advantage of openly-publicized cyber vulnerabilities. Trends in cybercrime are described, showing how malicious Internet websites, and other cybercrimes such as identity theft are linked to conventional terrorist activity.

Congress may wish to explore the possible effects on the U.S. economy and on the U.S. military that could result from a coordinated attack against civilian and military computers and communications systems, whether due to cybercrime or cyberterrorism. Congress may also wish to explore the difficulties associated with establishing doctrine for selecting an appropriate military or law enforcement response after such an attack.

[1] Dan Kuehl, professor at the National Defense University School of Information Warfare and Strategy, has pointed out that a high percentage of U.S. military messages flow through commercial communications channels, and this reliance creates a vulnerability during conflict. Eric Naef, "Wanja," *Infocon Magazine*, October 2003, http://www.iwar.org.uk/infocon/io-kuehl.htm.

[2] Sebastian Sprenger, "Maj. Gen. Lord Is a Groundbreaker," *Federal Computer Week*, October 15, 2007, vol. 21, no. 34, p. 44.

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

[4] Tim Greene, "Storm Worm Strikes Back at Security Pros," NetworkWorld.com, October 24, 2007, at http://www.networkworld.com/news/2007/102407-storm-worm-security.html?nlhtsec=1022securityalert4&&nladname=102507securityal.

[5] Brian Krebs, "Three Worked the Web to Help Terrorists," *The Washington Post*, July 6, 2007, p. D01. 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, at http://www2.gwu.edu/~bygeorge/060804/crimeterrorism.html.

Background

It is clear that terrorist groups are using computers and the Internet to further goals associated with spreading terrorism. This can be seen in the way that extremists are creating and using numerous Internet websites for recruitment and fund raising activities, and for Jihad training purposes. Several criminals who have recently been convicted of cybercrimes used their technical skills to acquire stolen credit card information in order to finance other conventional terrorist activities.[6] It is possible that as criminals and terrorist groups explore more ways to work together, a new type of threat may emerge where extremists gain access to the powerful network tools now used by cybercriminals to steal personal information, or to disrupt computer systems that support services through the Internet.

Three Basic Methods for Disrupting Computer Systems

There are several effective methods for disrupting computer systems. This report focuses on the method known as cyberattack, or computer network attack (CNA), which uses malicious computer code to disrupt computer processing, or steal data. A brief description of three different methods are shown here. However, as technology changes, future distinctions between these methods may begin to blur.

An attack against computers may (1) disrupt equipment and hardware reliability, (2) change processing logic, or (3) steal or corrupt data.[7] The methods discussed here are chosen based on the technology asset against which each attack mode is directed, and the effects each method can produce. The assets affected or effects produced can sometimes overlap for different attack methods.

- Conventional kinetic weapons can be directed against computer equipment, a computer facility, or transmission lines to create a physical attack that disrupts the reliability of equipment.
- The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse (EMP), can be used to create an electronic attack (EA) directed against computer equipment or data transmissions. By overheating circuitry or jamming communications, EA disrupts the reliability of equipment and the integrity of data.[8]
- Malicious code can be used to create a cyberattack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting a vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyberattack can

[6] Gregory Crabb, "U.S. Postal Service Global Investigations," and Yuval Ben-Itzhak, "CTO Finjan," Presentation at the Gartner IT Security Summit 2007, Washington, DC, June 4, 2007.

[7] All methods of computer attack are within the current capabilities of several nations. See CRS Report RL31787, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson.

[8] For more on electromagnetic weapons, see CRS Report RL32544, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*, by Clay Wilson.

disrupt the reliability of equipment, the integrity of data, and the confidentiality of communications.

Cyberattack, Cybercrime, and Cyberterrorism

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.[9] "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."

Definitions for Cyberterrorism

Various definitions exist for the term "cyberterrorism", just as various definitions exist for the term "terrorism."[10] 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."[11] 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."[12]

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.[13] 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."

Definitions for 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,

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

[10] 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.

[11] 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.

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

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

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 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.

Botnets

Botnets are becoming a major tool for cybercrime, partly because they can be designed to very effectively disrupt targeted computer systems in different ways, and because a malicious user, without possessing strong technical skills, can initiate these disruptive effects in cyberspace by simply renting botnet services from a cybercriminal.[14] Botnets, or "Bot Networks," are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code. Botnets have been described as the "Swiss Army knives of the underground economy" because they are so versatile.

Botnet designers, or "botmasters", can reportedly make large sums of money by marketing their technical services. For example, Jeanson Ancheta, a 21-year-old hacker and member of a group called the "Botmaster Underground", reportedly made more than $100,000 from different Internet Advertising companies who paid him to download specially-designed malicious adware code onto more than 400,000 vulnerable PCs he had secretly infected and taken over. He also made tens of thousands more dollars renting his 400,000-unit "botnet herd" to other companies that used them to send out spam, viruses, and other malicious code on the Internet. In 2006, Ancheta was sentenced to five years in prison.[15]

Botnet code was originally distributed as infected email attachments, but as users have grown more cautious, cybercriminals have turned to other methods. When users click to view a spam message, botnet code can be secretly installed on the users' PC. A website may be unknowingly infected with malicious code in the form of an ordinary-looking advertisement banner, or may include a link to an infected website. Clicking on any of these may install botnet code. Or, botnet code can be silently uploaded, even if the user takes no action while viewing the website, merely through some un-patched vulnerability that may exist in the browser. Firewalls and antivirus software do not necessarily inspect all data that is downloaded through browsers. Some bot software can even disable antivirus security before infecting the PC. Once a PC has been infected, the malicious software establishes a secret communications link to a remote "botmaster" in preparation to receive new commands to attack a specific target. Meanwhile, the malicious code may also automatically probe the infected PC for personal data, or may log keystrokes, and transmit the information to the botmaster.

The Shadowserver Foundation is an organization that monitors the number of command and control servers on the Internet, which indicates the number of bot networks that are being

[14] 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. Sebastian Sprenger, "Maj. Gen. Lord Is a Groundbreaker," *Federal Computer Week*, October 15, 2007, vol. 21, no. 34, p. 44.

[15] Bob Keefe, "PC Security Still More of a Wish than a Promise," *The Atlanta Journal*, February 3, 2007, p. 1A.

controlled online at a given time. From November 2006 through May 2007, approximately 1,400 command and control servers were found to be active on the Internet. The number of individual infected drones that are controlled by these 1,400 servers reportedly grew from half a million to more than 3 million from March to May 2007. Symantec, another security organization, reported that it detected 6 million bot-infected computers in the second half of 2006.[16]

Some botnet owners reportedly rent their huge networks for US$200 to $300 an hour, and botnets are becoming the weapon of choice for fraud and extortion.[17] Newer methods are evolving for distributing "bot" software that may make it even more difficult in the future for law enforcement to identify and locate the originating "botmaster." Some studies show that authors of software for botnets are increasingly using modern, open-source techniques for software development, including the collaboration of multiple authors for the initial design, new releases to fix bugs in the malicious code, and development of software modules that make portions of the code reusable for newer versions of malicious software designed for different purposes. This increase in collaboration among hackers mirrors the professional code development techniques now used to create commercial software products, and is expected to make future botnets even more robust and reliable. This, in turn, is expected to help increase the demand for malware services in future years.[18]

Traditionally, botnets organize themselves in an hierarchical manner, with a central command and control location (sometimes dynamic) for the botmaster. This central command location is useful to security professionals because it offers a possible central point of failure for the botnet. However, in the near future, security experts believe that attackers may use new botnet architectures that are more sophisticated, and more difficult to detect and trace. One class of botnet architecture that is beginning to emerge uses peer-to-peer protocol[19], which, because of its decentralized control design, is expected to be more resistant to strategies for countering its disruptive effects.[20] For example, some experts reportedly argue that a well-designed peer-to-peer botnet may be nearly impossible to shut down as a whole because it may provide anonymity to the controller, who can appear as just another node in the bot network.[21]

[16] Julie Bort, "Attack of the Killer Bots," *Network World*, Jul 2/9, 2007, p. 29.

[17] Susan MacLean, "Report warns of Organized Cyber Crime," *ItWorldCanada*, August 26, 2005, http://www.itworldcanada.com/a/IT-Focus/39c78aa4-df47-4231-a083-ddd1ab8985fb.html.

[18] McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf.

[19] Gnutella emerged as the first fully decentralized peer-to-peer protocol in 2000, and was used on the Internet to share and swap music files in MP3 compression format. The music industry was often frustrated in their efforts to counter this peer-to-peer technology because it could not identify a main controlling source. Since then, several other peer-to-peer protocols have been developed.

[20] Symantec, *Trojan.Peacomm: Building a Peer-to-Peer Botnet*, 2007, http://www.symantec.com/enterprise/security_response/weblog/2007/01/trojanpeacomm_building_a_peert.html. Matthew Broersma, *Peer-to-Peer Botnets a New and Growing Threat*, CSO Online, April 17, 2007, http://www2.csoonline.com/blog_view.html?CID=32852. Julian B. Grizzard et. al., *Peer-to-Peer Botnets: Overview and Case Study*, 2007, http://www.usenix.org/events/hotbots07/tech/full_papers/grizzard/grizzard_html/. Reinier Schoof and Ralph Koning, *Detecting Peer-to-Peer Botnets*, February 4, 2007, http://staff.science.uva.nl/~delaat/sne-2006-2007/p17/report.pdf.

[21] Tom Espiner, "Security Expert: Storm Botnet 'services' Could Be Sold," CnetNews.com, October 16, 2007, http://www.news.com/Security-expert-Storm-botnet-services-could-be-sold/2100-7349_3-6213781.html. Robert Lemos, *Bot software looks to improve peerage*, The Register, May 4, 2006, http://www.theregister.co.uk/2006/05/04/nugache_p2p_botnet/.

Estonia, 2007

In the Spring of 2007, government computer systems in Estonia experienced a sustained cyberattack that has been labeled by various observers as cyberwarfare, or cyberterror, or cybercrime. On April 27, officials in Estonia moved a Soviet-era war memorial commemorating an unknown Russian who died fighting the Nazis. The move stirred emotions, and led to 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 prime minister's Reform Party.[22]

In the early days of the cyberattack, government websites that normally receive around 1,000 visits a day reportedly were receiving 2,000 visits every second. This caused the repeated shut down of some websites for several hours at a time or longer, according to Estonian officials.[23] The attacks, which flooded computers and servers and blocked legitimate users, were described as crippling, owing to Estonia's high dependence on information technology, but limited resources for managing their infrastructure. Security experts say that the cyberattacks against Estonia were unusual because the rate of the packet attack was very high, and the series of attacks lasted weeks, rather than hour or days, which is more commonly seen for a denial of service attack.[24] Eventually, NATO and the United States sent computer security experts to Estonia to help recover from the attacks, and to analyze the methods used and attempt to determine the source of the attacks.

This event can serve to illustrate how computer network technology has blurred the boundaries between crime, warfare, and terrorism. A persistent problem during and after any cyberattack is accurate identification of the attacker, by finding out whether it was sponsored by a nation, or was the independent work of a few unconnected individuals, or was initiated by a group to instill frustration and fear by damaging the computerized infrastructure and economy. The uncertainty of not knowing the initiator also affects the decision about whom should ultimately become a target for retaliation, and whether the response should come from law enforcement or the military.

Initially, the Russian government was blamed by Estonian officials for the cyberattacks, and there were charges of cyberwarfare. Other observers argued that the cyberattack involved collusion between the Russian government and trans-national cybercriminals who made their large botnets available for short-term rent, either to individuals or to larger groups. They argue that as the rented time expired, the intensity of the persistent cyberattacks against Estonia also began to fall off.[25] However, not all security experts agree, and it remains unclear at this time whether the cyberattacks were sanctioned or initiated by the Russian government, or if a criminal botnet was actually involved.

[22] Robert Vamosi, "Cyberattack in Estonia—What It Really Means," CnetNews.com, May 29, 2007, at http://news.com.com/Cyberattack+in+Estonia-what+it+really+means/2008-7349_3-6186751.html.

[23] Christopher Rhoads, "Cyber Attack Vexes Estonia, Poses Debate," *The Wall Street Journal*, May 18, 2007, p. A6.

[24] Carolyn Marsan, "Examining the Reality of Cyberwar in Wake of Estonian Attacks," *Network World*, August 27, 2007, vol. 24, no. 33, p. 24.

[25] Iain Thomson, "Russia 'Hired Botnets' for Estonia Cyber-War," *Computing*, http://www.computing.co.uk/vnunet/news/2191082/claims-russia-hired-botnets.

After some investigation, network analysts later concluded that the cyberattacks targeting Estonia were not a concerted attack, but instead were the product of 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 war memorial was a very emotional topic for discussion. These analysts state that although access to various Estonian government agencies was blocked by the malicious code, there was no apparent attempt to target national critical infrastructure other than internet resources, and no extortion demands were made. Their analysis thus far concluded that there was no Russian government connection to the attacks against Estonia.[26] However, investigation into the incident continues, and officials from the United States view some aspects of the event as a possible model for future cyberwarfare or cyberterrorism directed against a nation state.

In January 2008, a court in Estonia convicted and fined a local man for bringing down a government website, as part of the extended cyberattack in 2007. The 20-year-old, who is apparently an ethnic Russian Estonian, used his home PC to carry out the attack. The investigation continues, and so far, he is the only person convicted for participating in the cyberattack against Estonia.[27]

Other Trends in Cybercrime Methods

Cybercrime is usually conducted through a connection to the Internet, but can also involve unauthorized removal of data on small, portable flash drive storage devices. Cybercrime, usually in the form of network hacking, has involved persons with strong technical skills, often motivated by the desire to gain popularity among their technology peers. However, the growing trend is now to profit from these network cyberattacks by targeting specific systems, often through collaboration among criminals and technical experts. The motives that drive these cybercriminal groups now may differ from those of their paying customers, who may possess little or no technical skills.

New technologies continue to outpace policy for law enforcement. Problems of coordination among agencies of different countries, along with conflicting national policies about crime in cyberspace, work to the advantage of cybercriminals who can choose to operate from geographic locations where penalties for some forms of cybercrime may not yet exist. Sophisticated tools for cyberattack can now be found for sale or for rent on the Internet, where highly-organized underground cybercrime businesses host websites that advertise a variety of disruptive software products and malicious technical services. High-end cybercrime groups use standard software business development techniques to keep their products updated with the latest anti-security features, and seek to recruit new and talented software engineering students into their organizations.

Where illicit profits are potentially very large, some high-end criminal groups have reportedly adopted standard IT business practices to systematically develop more efficient and effective computer code for cybercrime. Studies also show that organized crime groups now actively recruit college engineering graduates and technical expert members of computer societies, and

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

[27] Mike Sachoff, *Man Convicted In Estonia Cyber Attack*, WebProNews, January 24, 2008, http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack.

sponsor them to attend more information technology (IT) courses to further their technical expertise. However, in some cases, targeted students may not realize that a criminal organization is behind the recruitment offer.[28]

Cyberattacks are increasingly designed to silently steal information without leaving behind any damage that would be noticed by a user. These types of attacks attempt to escape detection in order to remain on host systems for longer periods of time. It is also expected that as mobile communication devices are incorporated more into everyday life, they will be increasingly targeted in the future for attack by cybercriminals.[29]

Malicious Code Hosted on Websites

Malicious code, such as viruses or Trojan Horses, are used to infect a computer to make it available for takeover and remote control. Malicious code can infect a computer if the user opens an email attachment, or clicks an innocent-looking link on a website. For example, users who visited the popular MySpace and YouTube websites in 2005, and who lacked important software security patches, reportedly may have had their PCs infected if they clicked on a banner advertisement which silently installed malicious code on their computers to log keystrokes or capture sensitive data. During the first half of 2006, the Microsoft Security Team reported that it had removed 10 million pieces of malicious software from nearly 4 million computers and web servers.[30] Recently, analysts at Google tested several million web pages for the presence of malicious software, and determined that 4.5 million of the web pages examined were suspicious in nature. After further testing of the 4.5 million web pages, over 1 million were found to launch downloads of malicious software, and more than two thirds of those programs were "bot" software that, among other things, collected data on banking transactions and then emailed the information to a temporary email account.[31]

Researchers at the San Jose, Calif.-based security firm, Finjan Inc., after reviewing security data from the first quarter of 2007, found that more malware is hosted on servers in countries such as the U.S. and U.K., than in other countries with less developed e-crime law enforcement policies. Findings from the Finjan 2007 Web Security Trends Report are based on an analysis of more than 10 million unique websites from Internet traffic recorded in the UK, and include the following:

- Attacks that involve the use of code obfuscation through diverse randomization techniques are growing more numerous and complex, making them virtually invisible to pattern-matching/signature-based methods in use by traditional antivirus products.

[28] McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf.

[29] A web crawler (also known as a Web spider or Web robot) is a program or automated script that browses the World Wide Web in a methodical, automated manner. Web crawlers are mainly used to create a copy of all the visited pages for later processing by a search engine that will index the downloaded pages to provide fast searches. Wikipedia, http://en.wikipedia.org/wiki/Web_crawler.

[30] Elise Ackerman, "Hackers' Infections Slither Onto Web Sites," *The Mercury News*, January 3, 2007, p. 1.

[31] Jeff Hecht, "Web Browsers Are New Frontline in Internet War," *NewScientistTech*, May 5, 2007, http://www.newscientisttech.com/article.ns?id=mg19426026.000&print=true. Niels Provos et. al., *The Ghost in the Browser: Analysis of Web-based Malware*, Google, Inc., http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf.

- Criminals are displaying an increasing level of sophistication when embedding malicious code within legitimate content with less dependence on outlaw servers in unregulated countries.

Finjan found that 90% of the websites examined containing malware resided on servers located in the U.S. or U.K. "The results of this study shatter the myth that malicious code is primarily being hosted in countries where e-crime laws are less developed," Finjan CTO Yuval Ben-Itzhak reportedly stated.[32]

Identity Theft

Botnets and other examples of malicious code can operate to assist cybercriminals with identity theft. 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 licences, birth certificates, reference letters, and bank statements.[33]

Identity theft involving thousands of victims is also enabled by inadequate computer security practices within organizations.[34] MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to U.S. consumers were accessed by computer hackers.[35] 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.[36] 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

[32] Finjan, Inc., *Web Security Trends Report, Q2 2007*, http://www.finjan.com/Content.aspx?id=827.

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

[34] 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.

[35] 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.

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

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.[37]

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 services for each stolen MasterCard number cost between $42 and $72.[38] 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.[39]

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.[40]

Cyber Espionage

Cyber espionage involves the unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files. However, should a terrorist group, nation, or other organization use computer hacking techniques for political or economic motives, their deliberate intrusions may also qualify them, additionally, as cybercriminals. If there is disagreement about this, it is likely because technology has outpaced policy for labeling actions in cyberspace. In fact, industrial cyber espionage may now be considered a necessary part of global economic competition, and secretly monitoring the computerized functions and capabilities of potential adversary countries may also be considered essential for national defense.[41]

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. Cyber espionage, which enables the exfiltration of massive amounts of information electronically, has now transformed the nature of counterintelligence, by enabling a reduced reliance on conventional spying operations.[42] The Internet, including satellite links and wireless local networks, now offers new, low cost and low

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

[38] 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/.

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

[40] 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.

[41] 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.

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

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 helps operate 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.[43]

Figure 1. Diagram of Purported Echelon Spy System

Source: BBC News, July 6, 2000, at http://news.bbc.co.uk/1/hi/world/europe/820758.stm.

The European parliament Special Committee reported that information gathered on Echelon may have helped the United States beat the European Airbus Consortium in selling aircraft to Saudi Arabia in 1994.[44] In 1995, France expelled five American diplomats and other officials, reportedly including the Paris station chief for the CIA, because of suspected industrial espionage activities linked to Echelon.[45]

The State Department denied that the U.S. government was engaged in industrial espionage. However, 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.[46]

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

[44] Ron Pemstein, "Europe Spy System," GlobalSecurity.org, March 30, 2000, http://www.globalsecurity.org/intell/library/news/2000/03/000330-echelon1.htm. Paul Meller, "European Parliament Adopts 'Echelon' Report," CNN.com, September 7, 2001, http://archives.cnn.com/2001/TECH/internet/09/07/echelon.report.idg/.

[45] Chris Marsden, "European Union to Investigate US-Run Satellite Spy Network," World Socialist Website, July 10, 2000, http://www.wsws.org/articles/2000/jul2000/eche-j10.shtml.

[46] European Parliament resolution on the existence of a global system for the interception of private and commercial (continued...)

Some government officials warn that criminals now sell or rent malicious code tools for cyber espionage, and the risk for damage to U.S. national security due to cyber espionage 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."[47]

In 2003, a series of cyberattacks designed to copy sensitive data files was launched against DOD systems, and the computers belonging to DOD contractors. The cyber espionage 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.[48] 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.[49]

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 cyber espionage 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.[50]

(...continued)

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.

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

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

[49] 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.

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

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 security attacks were reported globally during the first half of that year.[51] 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.[52]

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.[53]

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

[51] 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.

[52] 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.

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

to support terrorist groups.[54] 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 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.[55] 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.[56] Consequently, DEA officials reportedly argued that the war on drugs and the war against terrorism are and should be linked.[57]

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.[58] The poppy crop in Afghanistan reportedly supplies resin to produce over 90 percent 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.[59]

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

[54] 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.

[55] 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.

[56] 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.

[57] 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.

[58] 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.

[59] 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.

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.[60]

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.[61]

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.[62] 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

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

[61] 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.

[62] 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.

cyberattacks experienced in the near future by industrialized nations will be used by terrorist groups simply to supplement the more traditional physical terrorist attacks.[63]

Some observers have stated that Al Qaeda does not see cyberattack as important for achieving its goals, preferring attacks which inflict human casualties.[64] 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 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.[65] 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.[66]

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.[67] 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.[68]

Possible Effects of a Coordinated Cyberattack

In March 2007, researchers at Idaho National Laboratories (INL) conducted an experiment labeled the "Aurora Generator Test" to demonstrate the results of a simulated cyberattack on a power network. In a video released by the Department of Homeland Security, a power generator turbine, similar to many now in use throughout the United States, is forced to overheat and shut down dramatically, after receiving malicious commands from a hacker. The researchers at INL

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

[64] 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.

[65] 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.

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

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

[68] 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.

were investigating results of a possible cyberattack directed against a vulnerability that, reportedly, has since been fixed.[69] The video, however, implied that other multiple power generators sharing similar cyber vulnerabilities could potentially be disabled the same way.

In July 2002, the U.S. Naval War College hosted a war game called "Digital Pearl Harbor" to develop a scenario for a coordinated cyberterrorism event, where mock attacks by computer security experts against critical infrastructure systems simulated state-sponsored cyberwarfare. The simulated cyberattacks determined that the most vulnerable infrastructure computer systems were the Internet itself, and the computer systems that are part of the financial infrastructure.[70] It was also determined that attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because built-in system redundancy would prevent damage from becoming too widespread. The conclusion of the exercise was that a "Digital Pearl Harbor" in the United States was only a slight possibility.[71]

However, in 2002, a major vulnerability was discovered in switching equipment software that threatened the infrastructure for major portions of the Internet. A flaw in the Simple Network Management Protocol (SNMP) would have enabled attackers to take over Internet routers and cripple network telecommunications equipment globally. Network and equipment vendors worldwide raced quickly to fix their products before the problem could be exploited by hackers, with possible worldwide consequences. U.S. government officials also reportedly made efforts to keep information about this major vulnerability quiet until after the needed repairs were implemented on vulnerable Internet systems.[72] According to an assessment reportedly written by the FBI, the security flaw could have been exploited to cause many serious problems, such as bringing down widespread telephone networks and also halting control information exchanged between ground and aircraft flight control systems.[73]

Security experts agree that a coordinated cyberattack could be used to amplify the effects of a conventional terrorist attack, including a nuclear, biological, or chemical (NBC) attack. However, many of these same experts disagree about the damaging effects that might result from an attack

[69] Robert Lemos, *DHS Video Shows Potential Impact of Cyberattack*, SecurityFocus.com, September 27, 2007, http://www.securityfocus.com/brief/597.

[70] At the annual conference of the Center for Conflict Studies, Phil Williams, Director of the Program on Terrorism and Trans-National Crime and the University of Pittsburgh, said an attack on the global financial system would likely focus on key nodes in the U.S. financial infrastructure: Fedwire and Fednet. Fedwire is the financial funds transfer system that exchanges money among U.S. banks, while Fednet is the electronic network that handles the transactions. The system has one primary installation and three backups. "You can find out on the Internet where the backups are. If those could be taken out by a mix of cyber and physical activities, the U.S. economy would basically come to a halt," Williams said. "If the takedown were to include the international funds transfer networks CHIPS and SWIFT then the entire global economy could be thrown into chaos." George Butters, "Expect Terrorist Attacks on Global Financial System," October 10, 2003 at http://www.theregister.co.uk/content/55/33269.html.

[71] The simulation involved more than 100 participants. Gartner, Inc., "Cyberattacks: The Results of the Gartner/U.S. Naval War College Simulation," July 2002, at http://www3.gartner.com/2_events/audioconferences/dph/dph.html. War game participants were divided into cells, and devised attacks against the electrical power grid, telecommunications infrastructure, the Internet and the financial services sector. It was determined that "peer-to-peer networking," a special method of communicating where every PC used commonly available software to act as both a server and a client, posed a potentially critical threat to the Internet itself. William Jackson, "War College Calls Digital Pearl Harbor Doable," *Government Computer News*, August 23, 2002, at http://www.gcn.com/vol1_no1/daily-updates/19792-1.html.

[72] The vulnerability was found in Abstract Syntax Notation One (ASN.1) encoding, and was extremely widespread. Ellen Messmer, "President's Advisor Predicts Cyber-catastrophes Unless Security Improves," *Network World Fusion*, July 9, 2002 at http://www.nwfusion.com/news/2002/0709schmidt.html.

[73] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, June 27, 2002, p. A01.

directed against control computers that operate the U.S. critical infrastructure. Some observers have stated that because of U.S. dependency on computer technology, such attacks may have the potential to create economic damage on a large scale, while other observers have stated that U.S. infrastructure systems are resilient and would possibly recover easily, thus avoiding any severe or catastrophic effects.

While describing possible offensive tactics for military cyber operations, DOD officials reportedly stated that the U.S. could confuse enemies by using cyberattack to open floodgates, control traffic lights, or scramble the banking systems in other countries.[74] Likewise, some of China's military journals speculate that cyberattacks could disable American financial markets. China, however, is almost as dependent on these U.S. markets as the United States, and might possibly suffer even more from such a disruption to finances. As to using cyberattack against other U.S. critical infrastructures, the amount of potential damage that could be inflicted might be relatively trivial compared to the costs of discovery, if engaged in by a nation state. However, this constraint does not apply to non-state actors like Al Qaeda, thus making cyberattack a potentially useful tool for those groups who reject the global market economy.[75]

SCADA Vulnerabilities

Supervisory Control And Data Acquisition (SCADA) systems are the computers that monitor and regulate the operations of most critical infrastructure industries (such as the companies that manage the power grid). These SCADA computers automatically monitor and adjust switching, manufacturing, and other process control activities, based on digitized feedback data gathered by sensors. These control systems are often placed in remote locations, are frequently unmanned, and are accessed only periodically by engineers or technical staff via telecommunications links. However, for more efficiency, these communication links are increasingly connected to corporate administrative local area networks, or directly to the Internet.

Some experts believe that the importance of SCADA systems for controlling the critical infrastructure may make them an attractive target for terrorists.[76] Many SCADA systems also now operate using Commercial-Off-The-Shelf (COTS) software, which some observers believe are inadequately protected against a cyberattack. These SCADA systems are thought to remain persistently vulnerable to cyberattack because many organizations that operate them have not paid proper attention to these systems' unique computer security needs.[77]

[74] Sebastian Sprenger, "Maj.Gen. Lord Is a Groundbreaker," *Federal Computer Week*, October 15, 2007, vol. 21, no. 34, pp. 44-45.

[75] 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.

[76] Proprietary systems are unique, custom built software products intended for installation on a few (or a single) computers, and their uniqueness makes them a less attractive target for hackers. They are less attractive because finding a security vulnerability takes time, and a hacker may usually not consider it worth their while to invest the pre-operative surveillance and research needed to attack a proprietary system on a single computer. Widely used Commercial-Off-The-Shelf (COTS) software products, on the other hand, are more attractive to hackers because a single security vulnerability, once discovered in a COTS product, may be embedded in numerous computers that have the same COTS software product installed.

[77] Industrial computers sometimes have operating requirements that differ from business or office computers. For example, monitoring a chemical process, or a telephone microwave tower may require 24-hour continuous availability for a critical industrial computer. Even though industrial systems may operate using COTS software (see above), it may be economically difficult to justify suspending the operation of an industrial SCADA computer on a regular basis to (continued...)

The following example may serve to illustrate the possible vulnerability of control systems and highlight cybersecurity issues that could arise for infrastructure computers when SCADA controls are interconnected with office networks. In August 2003, the "Slammer"Internet computer worm was able to corrupt for five hours the computer control systems at the Davis-Besse nuclear power plant located in Ohio (fortunately, the power plant was closed and off-line when the cyberattack occurred). The computer worm was able to successfully penetrate systems in the Davis-Besse power plant control room largely because the business network for its corporate offices was found to have multiple connections to the Internet that bypassed the control room firewall.[78]

Other observers, however, suggest that SCADA systems and the critical infrastructure are more robust and resilient than early theorists of cyberterror have stated, and that the infrastructure would likely recover rapidly from a cyberterrorism attack. They cite, for example, that water system failures, power outages, air traffic disruptions, and other scenarios resembling possible cyberterrorism often occur as routine events, and rarely affect national security, even marginally. System failures due to storms routinely occur at the regional level, where service may often be denied to customers for hours or days. Technical experts who understand the systems would work to restore functions as quickly as possible. Cyberterrorists would need to attack multiple targets simultaneously for long periods of time to gradually create terror, achieve strategic goals, or to have any noticeable effects on national security.[79]

For more information about SCADA systems, see CRS Report RL31534, *Critical Infrastructure: Control Systems and the Terrorist Threat*, by Dana A. Shea.

Unpredictable Interactions Between Infrastructures

An important area that is not fully understood concerns the unpredictable interactions between computer systems that operate the different U.S. infrastructures. The concern is that numerous interdependencies (where downstream systems may rely on receiving good data through stable links with upstream computers) could possibly build to a cascade of effects that are unpredictable in how they might affect national security.[80] For example, while the "Blaster" worm was disrupting Internet computers over several days in August 2003, some security experts suggest that slowness of communication links, caused by Blaster worm network congestion, may have contributed to the Eastern United States power blackout that occurred simultaneously on August 14. The computer worm could have degraded the performance of several communications links

(...continued)

take time to install every new security software patch. See interview with Michael Vatis, director of the Institute for Security Technology Studies related to counterterrorism and cybersecurity. Sharon Gaudin, "Security Experts: U.S. Companies Unprepared for Cyber Terror," *Datamation*, July 19, 2002 at http://itmanagement.earthweb.com/secu/article.php/1429851. Also, Government Accountability Office, *Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD*, GAO-03-1037T, July 24, 2003, p. 8.

[78] Kevin Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Network," *Security Focus*, August 19, 2003, at http://www.securityfocus.com/news/6767.

[79] Scott Nance, "Debunking Fears: Exercise Finds 'Digital Pearl Harbor' Risk Small," *Defense Week*, April 7, 2003 at http://www.kingpublishing.com/publications/dw/.

[80] The most expensive natural disaster in U.S. history, Hurricane Andrew, is reported to have caused $25 billion in damage, while the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. However, the Love Bug virus was created and launched by a single university student in the Philippines, relying on inexpensive computer equipment. Christopher Miller, *GAO Review of Weapon Systems Software*, March 3, 2003, e-mail communication, MillerC@gao.gov.

between data centers normally used to send warnings to other utility managers downstream on the power grid.[81]

Civilian Technology that Supports DOD

DOD uses Commercial-Off-The-Shelf (COTS) hardware and software products in core information technology administrative functions, and also in the combat systems of all services, as for example, in the integrated warfare systems for nuclear aircraft carriers.[82] DOD favors the use of COTS products in order to take advantage of technological innovation, product flexibility and standardization, and resulting contract cost-effectiveness. Nevertheless, DOD officials and others have stated that COTS products are lacking in security, and that strengthening the security of those products to meet military requirements may be too difficult and costly for most COTS vendors. To improve security, DOD Information Assurance practices require deploying several layers of additional protective measures around COTS military systems to make them more difficult for enemy cyberattackers to penetrate.[83]

However, on two separate occasions in 2004, viruses reportedly infiltrated two top-secret computer systems at the Army Space and Missile Defense Command. It is not clear how the viruses penetrated the military systems, or what the effects were. Also, contrary to security policy requirements, the compromised computers reportedly lacked basic anti virus software protection.[84] Security experts have noted that no matter how much protection is given to computers, hackers are always creating new ways to defeat those protective measures.[85]

Why Cyberattacks Are Successful

Networked computers with exposed vulnerabilities may be disrupted or taken over by a hacker, or by automated malicious code. Botnets opportunistically scan the Internet to find and infect computer systems that are poorly configured, or lack current software security patches. Compromised computers are taken over to become slaves in a "botnet", which can include thousands of compromised computers that are remotely controlled to collect sensitive information from each victim's PC, or to collectively attack as a swarm against other targeted computers.

Even computers that have updated software and the newest security patches may still be vulnerable to a type of cyberattack known as a "Zero-Day exploit." This may occur if a computer

[81] Network congestion caused by the Blaster worm reportedly delayed the exchange of critical power grid control data across the public telecommunications network, which could have hampered the operators' ability to prevent the cascading effect of the blackout. Dan Verton, "Blaster Worm Linked to Severity of Blackout," *Computerworld*, August 29, 2003, http://www.computerworld.com/printthis/2003/0,4814,84510,00.html.

[82] Some ships of the U.S. Navy use Windows software. Bill Murray, "Navy Carrier to Run Win 2000," *GCN.com*, September 11, 2000, http://www.gcn.com/vol19_no27/dod/2868-1.html. Major U.K. naval systems defense contractor, BAE Systems, also took the decision to standardize future development on Microsoft Windows. John Lettice, "OSS Torpedoed: Royal Navy Will Run on Windows for Warships," *Register*, September 6, 2004 at http://www.theregister.co.uk/2004/09/06/ams_goes_windows_for_warships/.

[83] Patience Wait, "Defense IT Security Can't Rest on COTS," *GCN.com*, September 27, 2004, at http://www.gcn.com/23_29/news/27422-1.html.

[84] Dawn Onley, "Army Urged to Step Up IT Security Focus," *GCN.com*, September 2, 2004, at http://www.gcn.com/vol1_no1/daily-updates/27138-1.html.

[85] Patience Wait, "Defense IT Security Can't Rest on COTS," *GCN.com*, September 27, 2004, at http://www.gcn.com/23_29/news/27422-1.html.

hacker discovers a new software vulnerability and launches a malicious attack to infect computers before a security patch can be created by the software vendor and distributed to protect users. Zero-day vulnerabilities in increasingly complex software are regularly discovered by computer hackers. Recent news articles report that zero-day vulnerabilities are now available at online auctions, where buyers and sellers negotiate with timed bidding periods and minimum starting prices. This allows newly-discovered computer security vulnerabilities to be sold quickly to the highest bidder. Computer security expert Terri Forslof, of Tipping Point, has reportedly said that such practices will "...increase the perceived value of vulnerabilities, and the good guys already have trouble competing with the money you can get on the black market."[86]

The Insider Threat

A major threat for organizations is the ease with which data can now be copied and carried outside using a variety of portable storage devices, such as small flash drives. Newer high-density memory stick technology reportedly allows installed computer applications to be run entirely from the flash drive. This means that the entire contents of a PC could possibly be copied to and stored on a small, easily portable, and easily concealed media device.[87]

Employees with access to sensitive information systems can initiate threats in the form of malicious code inserted into software that is being developed either locally, or under offshore contracting arrangements. For example, in January 2003, 20 employees of subcontractors working in the United States at the Sikorsky Aircraft Corporation were arrested for possession of false identification used to obtain security access to facilities containing restricted and sensitive military technology. All of the defendants pleaded guilty and have been sentenced, except for one individual who was convicted at trial on April 19, 2004.[88]

Persistence of Computer System Vulnerabilities

Vulnerabilities in software and computer system configurations provide entry points for a cyberattack. Vulnerabilities persist largely as a result of poor security practices and procedures, inadequate training in computer security, or technical errors in software products.[89] Inadequate resources devoted to staffing the security function may also contribute to poor security practices. Home PC users often have little or no training in best practices for effectively securing home networks and equipment.

Errors in New Software Products

Vendors for Commercial-Off-The-Shelf software (COTS) are often criticized for releasing new products with errors that create the computer system vulnerabilities.[90] Richard Clarke, former

[86] Tim Green, *Web Site auctions software vulnerabilities to highest bidder*, Network World, August 8, 2007.

[87] McAfee Virtual Criminology Report: Organized Crime and the Internet, December 2006, http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf.

[88] U.S. Attorneys Office, District of Connecticut, at http://www.usdoj.gov/usao/ct/attf.html.

[89] The SANS Institute, in cooperation with the National Infrastructure Protection Center (NIPC), publishes an annual list of the 10 most commonly exploited vulnerabilities for Windows systems and for Unix systems. *The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities, 2003*, SANS, April 15, 2003 at http://www.sans.org/top20/.

[90] In September 2003, Microsoft Corporation announced three new critical flaws in its latest Windows operating (continued...)

White House cyberspace advisor until 2003, has reportedly said that many commercial software products have poorly written, or poorly configured security features.[91] In response to such criticism, the software industry reportedly has made new efforts to design products with architectures that are more secure. For example, Microsoft has created a special Security Response Center and now works with DOD and with industry and government leaders to improve security features in its new products. However, many software industry representatives reportedly agree that no matter what investment is made to improve software security, there will continue to be vulnerabilities in future software because products are becoming increasingly more complex.[92]

Inadequate Resources

Although software vendors periodically release fixes or upgrades to solve newly discovered security problems, an important software security patch might not get scheduled for installation on an organization's computers until several weeks or months after the patch is available.[93] The job may be too time-consuming, too complex, or too low a priority for the system administration staff. With increased software complexity comes the introduction of more vulnerabilities, so system maintenance is never-ending. Sometimes the security patch itself may disrupt the computer when installed, forcing the system administrator to take additional time to adjust the computer to accept the new patch. To avoid such disruption, a security patch may first require testing on a separate isolated network before it is distributed for installation on all other regular networked computers.

Because of such delays, the computer security patches installed in many organizations may lag considerably behind the current cyberthreat situation. Whenever delays are allowed to persist in private organizations, in government agencies, or among PC users at home, computer vulnerabilities that are widely reported may remain unprotected, leaving networks open to possible attack for long periods of time.

(...continued)

systems software. Security experts predicted that computer hackers may possibly exploit these new vulnerabilities by releasing more attack programs, such as the "Blaster worm" that recently targeted other Windows vulnerabilities causing widespread disruption on the Internet. Jaikumar Vijayan, "Attacks on New Windows Flaws Expected Soon," *Computerworld*, September 15, 2003, vol. 37, no. 37, p. 1.

[91] Agencies operating national security systems must purchase software products from a list of lab-tested and evaluated products in a program that requires vendors to submit software for review in an accredited lab, a process (known as certification and accreditation under the Common Criteria, a testing program run by the National Information Assurance Partnership) that often takes a year and costs several thousand dollars. The review requirement previously has been limited to military national security software, however, the administration has stated that the government will undertake a review of the program in 2003 to "possibly extend" it as a new requirement for civilian agencies. Ellen Messmer, White House issue "National Strategy to Secure Cyberspace," *Network World Fusion*, February 14, 2003, http://www.nwfusion.com/news/2003/0214ntlstrategy.html.

[92] Scott Charney, Chief Security Strategist, Microsoft, Statement before the House Committee on Armed Services, Terrorism, Unconventional Threats and Capabilities Subcommittee, *Information Technology in the 21st Century Battlespac*e, hearing, July 24, 2003, p. 9.

[93] A survey of 2000 PC users found that 42% had not downloaded the vendor patch to ward off the recent Blaster worm attack, 23% said they do not regularly download software updates, 21% do not update their anti-virus signatures, and 70% said they were not notified by their companies about the urgent threat due to the Blaster worm. Jaikumar Vijayan, "IT Managers Say They Are Being Worn Down by Wave of Attacks," *Computerworld*, August 25, 2003, vol. 37, no. 34, p. 1.

Future Attractiveness of Critical Infrastructure Systems

There has yet been no published evidence showing a widespread focus by cybercriminals on attacking the control systems that operate the U.S. civilian critical infrastructure. Disabling infrastructure controls for communications, electrical distribution or other infrastructure systems, is often described as a likely scenario to amplify the effects of a simultaneous conventional terrorist attack involving explosives.

However, in 2006, at a security discussion in Williamsburg, Virginia, a government analyst reportedly stated that criminal extortion schemes may have already occurred, where cyberattackers have exploited control system vulnerabilities for economic gain. And, in December 2006, malicious software that automatically scans for control system vulnerabilities reportedly was made available on the Internet for use by cybercriminals. This scanner software reportedly can enable individuals with little knowledge about infrastructure control systems to locate a SCADA computer connected to the Internet, and quickly identify its security vulnerabilities.

The Idaho National Laboratory is tasked to study and report on technology risks associated with infrastructure control systems. Past studies have shown that many, if not most, automated control systems are connected to the Internet, or connected to corporate administrative systems that are connected to the Internet, and are currently vulnerable to a cyberattack. And, because many of these infrastructure SCADA systems were not originally designed with security as a priority, in many cases, new security controls cannot now be easily implemented to reduce the known security vulnerabilities.[94] Following past trends, where hackers and cybercriminals have taken advantage of easy vulnerabilities, some analysts now predict that we may gradually see new instances where cybercriminals exploit vulnerabilities in critical infrastructure control systems.[95]

Measuring Cybercrime

New, automated attack methods have outpaced current methods for tracking the number and severity of cyberattacks and cybercrime intrusions. For example, according to a study by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") automatically spread to infect more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest-spreading computer worm in history. As the study reports, the Slammer worm doubled in size every 8.5 seconds and achieved its full scanning rate (55 million scans per second) after about 3 minutes. It caused considerable harm through network outages which led to numerous canceled airline flights and automated teller machine (ATM) failures.[96]

[94] Testimony of Aaron Turner, House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity and Science & Technology, Hearing on "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure," April 19, 2007, http://homeland.house.gov/SiteDocuments/20070419153130-95132.pdf.

[95] Testimony of Aaron Turner, House Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity and Science & Technology, Hearing on "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure," April 19, 2007, http://homeland.house.gov/SiteDocuments/20070419153130-95132.pdf.

[96] "Internet Worm Keeps Striking," January 27, 2003, *CBSNews.com* at http://www.cbsnews.com/stories/2003/01/28/tech/main538200.shtml.

The use of automated tools for cybercrime has had a dramatic affect on the Computer Emergency Response Team/ Coordinating Center (CERT/CC). In 2004, CERT/CC announced that it had abandoned its traditional practice of producing an annual report tracking the number of cyber intrusions recorded for each year. For many years prior to 2004, CERT/CC had maintained a database of statistics about security incidents that were reported to it anonymously by businesses and individuals worldwide. The reason given for abandoning its annual tracking report was because the widespread use of new, automated cyberattack tools had escalated the number of network attacks to such a high level, that the CERT/CC organization determined that traditional methods for counting security incidents had become meaningless as a metric for assessing the scope and effects of attacks against Internet-connected systems.[97] The CERT-CC website currently states, "Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, beginning in 2004, we stopped publishing the number of incidents reported."[98]

The FBI estimates that all types of computer crime in the U.S. now costs industry about $400 billion, while officials in the Department of Trade and Industry in Britain say computer crime has risen by 50 percent from 2005 to 2006. As one example of costs associated with a recent computer security breach, TJX, the parent company of TJ Maxx, took a $12 million charge in its fiscal first quarter of 2008 due to the theft of more than 45 million credit and debit card numbers, starting in 2006. The money reportedly went to investigating and containing the intrusion, improving computer security, communicating with customers, and other fees. TJX estimates that, adding damages from future lawsuits, the breach may eventually cost $100 per lost record, or a total of $4.5 billion.[99]

It is estimated that only five per cent of cybercriminals are ever arrested or convicted because the anonymity associated with web activity makes them hard to catch, and the trail of evidence needed to link them to a cybercrime is hard to unravel. Studies also show that cybercrime incidents are rarely reported, especially by companies that wish to avoid negative publicity leading to possible loss of confidence by its customers. However, law enforcement officials argue that "maintaining a code of silence" won't benefit a company in the long-run. Steven Martinez, deputy assistant director for the FBI's cyber division, reportedly stated at the 2006 RSI Computer Security Conference that partnerships between law enforcement, the academic community, and the private sector are key to understanding and reducing cybercrime.[100]

Each year, the Computer Security Institute (CSI), with help from the FBI, conducts a survey of thousands of security practitioners from U.S. corporations, government agencies, financial institutions, and universities. The CSI/FBI Computer Crime and Security Survey, published annually, is perhaps the most widely-used source of information about how often computer crime occurs and how expensive these crimes can be. The 2006 survey indicated that the average financial loss reported due to security breaches was $167,713, an 18% decrease from the previous year's average loss of $203,606.

[97] "CERT/CC Statistics 1988-2004" at http://www.cert.org/stats/cert_stats.html.

[98] CERT Coordination Center, Carnegie Mellon University, http://www.cert.org/stats/.

[99] Sharon Gaudin, *Breach Costs Soar at TJX*, Information Week, May 21, 2007, p. 19.

[100] Marcia Savage, "Companies Still Not Reporting Attacks, FBI Director Says," SearchSecurity.com, February 15, 2006, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1166845,00.html?bucket=NEWS&topic=299990.

However, some observers argue that the analyses reported in the CSI/FBI survey may be questionable, because the survey methodology is not statistically valid.[101] This is because the survey is limited only to CSI members, which reduces the likelihood that respondents are a representative sample of all security practitioners, or that their employers are representative of employers in general. In addition, the 2006 CSI/FBI survey points out that most companies are continuing to sweep security incidents under the rug.

With the apparent absence of statistically valid survey results concerning the financial costs of computer crime, and with an accompanying lack of clear data about the number and types of computer security incidents reported, it appears that there may be no valid way to currently understand the real scope and intensity of cybercrime. The growing use of botnets and sophisticated malicious code also suggests that the percentage of unreported cybercrime, plus the percentage undetected, may both be going up.

Problems Tracing Cybercrime

The challenge of identifying the source of attacks is complicated by the unwillingness of commercial enterprises to report attacks, owing to potential liability concerns. CERT/CC estimates that as much as 80% of all actual computer security incidents still remain unreported.[102] Law enforcement officials concede they are making little progress in tracing the profits and finances of cybercriminals. Online payment services, such as PayPal and E-Gold, enable criminals to launder their profits and exploit the shortcomings of international law enforcement. Recently, Intermix Media was fined $7.5 million in penalties for distribution of spyware which silently captures personal information from user's PCs. However, some adware and spyware purveyors reportedly can still make millions of dollars per year in profits. Many companies who distribute spyware are difficult to pursue legally because they typically also offer some legitimate services. In many cases, the finances that back cybercrimes are so distributed they are hard for law enforcement to figure out.[103]

Organized Cybercrime

Some large cybercriminal groups are transnational, with names like Shadowcrew, Carderplanet, and Darkprofits. Individuals in these groups reportedly operate from locations all over the world, working together to hack into systems, steal credit card information and sell identities, in a very highly structured, organized network.[104] Organized crime is also recruiting teenagers who indicate they feel safer doing illegal activity online than in the street. A recent report from the McAfee security organization, titled the "Virtual Criminology Report", draws on input from Europe's leading high-tech crime units and the FBI, and suggests that criminal outfits are targeting top

[101] Bill Brenner, "Security Blog Log: Has CSI/FBI Survey Jumped the Shark?" SearchSecurity.com, July 21, 2006, http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1202328,00.html.

[102] Many cyberattacks are unreported usually because the organization is unable to recognize that it has been attacked, or because the organization is reluctant to reveal publicly that it has experienced a cyberattack, Government Accountability Office, *Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD*, GAO-03-1037T, July 24, 2003, p. 6.

[103] Matt Hines, "Malware Money Though to Trace," *Eweek*, September 18, 2006, p. 14.

[104] Kevin Poulsen, "Feds Square off with Organized Cyber Crime," SecurityFocus, February 17, 2005, http://www.securityfocus.com/news/10525.

students from leading academic institutions and helping them acquire more of the skills needed to commit high-tech crime on a massive scale.[105]

In the future, we may see new and different modes of criminal organization evolve in cyberspace. Cyberspace frees individuals from many of the constraints that apply to activities in the physical world, and current forms of criminal organization may not transition well to online crime. Cybercrime requires less personal contact, less need for formal organization, and no need for control over a geographical territory. Therefore, some researchers argue that the classical hierarchical structures of organized crime groups may be unsuitable for organized crime on the Internet. Consequently, online criminal activity may emphasize lateral relationships and networks instead of hierarchies.[106]

Instead of assuming stable personnel configurations that can persist for years, online criminal organization may incorporate the "swarming" model, in which individuals coalesce for a limited period of time in order to conduct a specific task, or set of tasks, and afterwards go their separate ways. The task of law enforcement could therefore become much more difficult. If cybercriminals evolve into the "Mafia of the moment" or the "cartel of the day," police will lose the advantage of identifying a permanent group of participants who engage in a set of routine illicit activities, and this will only contribute to the future success of organized cybercrime.[107]

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.[108] In 2003, the National Strategy to Secure Cyberspace was published by the 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.[109]

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

[105] Bill Brenner, "Criminals Find Safety in Cyberspace," SearchSecurity.com, December 18, 2006, http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1235455,00.html?bucket=NEWS&topic=299990.

[106] Council of Europe Octopus Programme, *Summary of the Organised Crime Situation Report 2004: Focus on the Threat of Cybercrime*, Strausbourg, September 6, 2004, p. 48.

[107] Susan Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships," *North Carolina Journal of Law and Technology*, 2002, http://www.jolt.unc.edu/Vol4_I1/Web/Brenner-V4I1.htm.

[108] 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.

[109] 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.

addition, a new Cyber Warning and Information Network (CWIN) has begun operation in 50 locations, and serves as an early warning system for cyberattacks.[110] 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.[111]

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.[112]

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 first and only international treaty to deal 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.[113]

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 would raise Constitutional issues in the United States.[114] 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. 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."[115]

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

[111] 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.

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

[113] 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.

[114] 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.

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

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.[116]

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.[117] 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.[118] In 2007, the Government Accountability Office issued a report, titled "Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but 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.[119] 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.

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

[117] 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.

[118] 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.

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

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.[120]

Issues for Congress

Policy issues for cybercrime and cyberterrorism include a need for the following:

- increase awareness about changing threats due to the growing technical skills of extremists and terrorist groups;
- develop more accurate methods for measuring the effects of cybercrime;
- help to determine appropriate responses by DOD to a cyberattack;
- examine the incentives for achieving the goals of the National Strategy to Secure Cyberspace;
- 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.

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.[121]

Growth in Technical Capabilities of Terrorists

Seized computers belonging to Al Qaeda indicate its members are becoming more familiar with hacker tools and services that are available over the Internet.[122] Could terrorist groups find it advantageous to hire a cybercrime botnet tailored to attack specific targets, possibly including the

[120] 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.

[121] 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.

[122] Richard Clarke, "Vulnerability: What Are Al Qaeda's Capabilities?" *PBS Frontline: Cyberwar*, April 2003, at http://www.pbs.org.

civilian critical infrastructure of Western nations? Could cybercrime botnets, used strategically, provide a useful way for extremists to amplify the effects of a conventional terrorist attack using bombs?

As computer-literate youth increasingly join the ranks of terrorist groups, will cyberterrorism likely become increasingly more mainstream in the future? Will a computer-literate leader bring increased awareness of the advantages of an attack on information systems, or be more receptive to suggestions from other, newer computer-literate members? Once a new tactic has won widespread media attention, will it likely motivate other rival terrorist groups to follow along the new pathway?[123]

Better Measurement of Cybercrime Trends

Experiences at CERT/CC show that statistical methods for measuring the volume and economic effects of cyberattacks may be questionable. Without sound statistical methods to accurately report the scope and effects of cybercrime, government and legal authorities will continue to have unreliable measures of the effectiveness of their policies and enforcement actions.

Figures from several computer security reports now used for measuring annual financial losses to U.S. industry due to intrusions and cybercrime are believed by some observers to be limited in scope or possibly contain statistical bias.[124] Is there a need for a more statistically reliable analysis of trends in computer security vulnerabilities and types of cyberattacks to more accurately show the costs and benefits for improving national cybersecurity? Congress may wish to encourage security experts to find more effective ways to collect data that will enable accurate analysis of trends for cyberattacks and cybercrime. Congress may also wish to encourage security researchers to find better ways to identify the initiators of cyberattacks.

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 must 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

[123] Jerrold M. Post, Kevin G. Ruby, and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat From Information Terrorism," *Terrorism and Political Violence*, summer 2000, vol. 12, no. 2, pp. 97-122.

[124] A well known source of information about the costs of cyberattacks is the annual computer security survey published by the Computer Security Institute (CSI), which utilizes data collected by the FBI. However, respondents to the CSI/FBI survey of computer security issues are generally limited only to CSI members, which may create statistical bias that affects the survey findings. Recently, CSI has also conceded weaknesses in its analytical approach and has suggested that its survey of computer security vulnerabilities and incidents may be more illustrative than systematic. However, the CSI/FBI survey remains useful despite its imperfect methodology. Bruce Berkowitz and Robert W. Hahn, "Cybersecurity: Who's Watching the Store?" *Issues in Science and Technology*, spring 2003.

countries that are U.S. allies, or even turned back to attack civilian computer systems in the United States?[125] If the effects become widespread and severe, could the U.S. use of cyberweapons exceed the customary rules of military conflict, or violate international laws.[126]

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.[127] 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 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.[128]

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?[129] Would regulation to improve computer security interfere with innovation and

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

[126] 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.

[127] 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.

[128] 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.

[129] 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 (continued...)

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 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.[130]

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, 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.[131] 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

(...continued)

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.

[130] 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 reponds 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.

[131] 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.

requires sharing of relevant information about threats, vulnerabilities, and exploits.[132] 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? And, 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 publicity and guard their trade secrets?[133] 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.[134] 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.[135]

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

H.R. 1525—The Internet Spyware (I-SPY) Prevention Act of 2007, proposes penalties for unauthorized access to computers, or the use of computers to commit crimes. 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 establishes 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 directs the Assistant Secretary to do the following:

---

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

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

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

[135] 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.

- 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.
- 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.

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

H.R. 3221—The New Direction for Energy Independence, National Security, and Consumer Protection Act proposes establishment of the Grid Modernization Commission to facilitate the adoption of Smart Grid standards, technologies, and practices across the Nation's electricity grid. The bill was passed in the House on August 4, 2007. On October 19, 2007, there was a unanimous consent request to consider H.R. 3221 in the Senate, but objection was heard.

H.R. 3237—The Smart Grid Facilitation Act of 2007, proposes to modernize the Nation's electricity transmission and distribution system to incorporate digital information and controls technology. "Smart grid" technology functions will include the ability to detect, prevent, respond to, or recover from cyber-security threats and terrorism. The new Grid Modernization Commission is 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.

Author Contact Information

Clay Wilson
Specialist in Military Information Technology
cwilson@crs.loc.gov, 7-8748