Order Code RL32114

CRS Report for Congress
Received through the CRS Web

Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress

October 17, 2003

Clay Wilson
Specialist in Technology and National Security
Foreign Affairs, Defense, and Trade Division

Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress

Summary

Persistent computer security vulnerabilities may expose U.S. critical infrastructure and government computer systems to possible cyber attack by terrorists, possibly affecting the economy or other areas of national security. This report discusses possible cyber capabilities of terrorists and sponsoring nations, describes how computer security vulnerabilities might be exploited through a cyber terror attack, and raises some potential issues for Congress.

Currently no evidence exists that terrorist organizations are actively planning to use computers as a means of attack, and there is disagreement among some observers about whether critical infrastructure computers offer an effective target for furthering terrorists' goals. However, terrorist organizations now use the Internet to communicate, and news reports have indicated that Al Qaeda and other groups may be using computer technology to help plan future terrorist attacks. At the same time, nuisance attacks against computer systems and the Internet are becoming more rapid and widespread, indicating that computer system vulnerabilities persist despite growing concerns about possible effects on national security.

This report presents a working definition for the term "cyber terrorism", plus background information describing how current technology and management processes may leave computers exposed to cyber attack, and a discussion of possible effects of a cyber attack. Potential issues for Congress are presented in the second section, including: whether appropriate guidance exists for a DOD information warfare response to a cyber attack; whether the need to detect possible cyber terrorist activity interferes with individual privacy; whether the roles and responsibilities for protecting against a possible cyber terrorist attack need more clarity for government, industry, and home users; and, whether information sharing on cyber threats and vulnerabilities must be further increased between private industry and the federal government. The final section describes possible policy options for improving protection against threats from possible cyber terrorism.

Appendices to this report explain technologies underlying computer viruses, worms, and spyware, how these malicious programs enable cyber crime and cyber espionage, and how tactics currently used by computer hackers might also be employed by terrorists while planning a possible cyber terror attack.

This report will be updated to accommodate significant changes.

Contents

Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress

Introduction

Many Pentagon officials reportedly believe that future adversaries may be unwilling to array conventional forces against U.S. troops, and instead may resort to "asymmetric warfare"[1], where a less powerful opponent uses other strategies to offset and negate U.S. technological superiority. Also, partly because the U.S. military relies significantly on the civilian information infrastructure, these officials believe that future conflicts may be characterized by a blurring in distinction between civilian and military targets.[2] As a consequence, they believe that government and civilian computers and information systems are increasingly becoming a viable target for opponents of the U.S., including international terrorist groups.

Terrorist groups today frequently use the Internet to communicate, raise funds, and gather intelligence on future targets. Although there is no published evidence that computers and the Internet have been used directly, or targeted in a terrorist attack,[3] malicious attack programs currently available through the Internet can allow anyone to locate and attack networked computers that have security vulnerabilities, and possibly disrupt other computers without the same vulnerabilities. Terrorists could also use these same malicious programs, together with techniques used by computer hackers (see Appendix A), to possibly launch a widespread cyber attack against computers and information systems that support the U.S. critical infrastructure.

Some security experts believe that past discussions about cyber terrorism may have over-inflated the perceived risk to the critical infrastructure.[4] However, other

---

[1] According to Pentagon officials, the supporting infrastructure (power grid, phone network, the Internet, etc.) for United States technology would likely become a target for asymmetric warfare attack. Jonathan B. Tucker, 1999, *Asymmetric Warfare*, Forum for Applied Research and Public Policy, vol. 14, no. 2.

[2] 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.

[3] John Arquilla and David Ronfeldt, *The Advent of Netwar (Revisited)*, Networks and Netwars: The Future of Terror, Crime and Militancy, Rand, Santa Monica, 2001, p. 1-28.

[4] The critical infrastructure is viewed by some as more resilient than previously thought to

(continued...)

observers believe that security threats are continuously evolving along with changes in technology. They believe that terrorist groups are recruiting new, younger members more knowledgeable about computer technology, and that some day a terrorist group may attempt to use computers as a weapon.

The Background section of this report presents a working definition of cyber terrorism, and describes how persistent vulnerabilities in computer systems operated by government, industry, and home PC users enable computer attacks to be successful. The next section presents potential issues for Congress pertaining to the risks of cyber terrorism. The final section presents policy options addressing related issues. Three appendices describe, in more detail, the technology and tactics used in a computer attack.

Background

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 civilian federal agencies.[5] 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.[6]

The Department of Homeland Security (DHS) has created the National Cyber Security Division (NCSD) under the Department's Information Analysis and Infrastructure Protection Directorate.[7] The NCSD oversees a Cyber Security Tracking, Analysis and Response Center (CSTARC) which is tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and warnings for cyber threats, improving information sharing, responding to major cyber security incidents, and aiding in national-level recovery efforts. In addition, a new Cyber

---

[4] (...continued)
the effects of a computer attack. Drew Clark, June 3, 2003, *Computer Security Officials Discount Chances of 'Digital Pearl Harbor'*, [http://www.GovExec.com.]

[5] 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.

[6] Tinabeth Burton, May 7, 2003, *ITAA Finds Much to Praise in National Cybersecurity Plan*, [http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1045252973]

[7] DHS is comprised of five major divisions or directorates: Border & Transportation Security; Emergency Preparedness & Response; Science & Technology; Information Analysis & Infrastructure Protection; and Management. See [http://www.dhs.gov/dhspublic/display?theme=52.]

Warning and Information Network (CWIN) has begun operation in 30 locations, and serves as an early warning system for cyber attacks.[8]

In January 2003, the administration announced the creation of a new Terrorist Threat Integration Center (TTIC) to monitor and analyze threat information gathered by other agencies. Leadership for TTIC comes from senior officers of the CIA, FBI, DOD, DHS and the Department of State, which are the component agencies of the TTIC. The TTIC itself has no independent authority to collect intelligence, and instead operates by combining the data elements and information on trans-national terrorist activity collected by component agencies. Some observers have suggested that the TTIC should be housed within the DHS, rather than within the CIA, in order to eliminate possible cultural and constitutional conflicts between the CIA and the FBI.[9]

However, despite growing concerns for national security, computer vulnerabilities persist, the number of computer attacks reported by industry and government has increased every year, and federal agencies have, for the past 2 years, come under criticism for the effectiveness of their computer security programs.[10] In addition, a study by one computer security organization found that, during the latter half of 2002, the highest rates for global computer attack activity were directed against critical infrastructure industry companies, such as power, energy, and financial services.[11] In January 2003, an Internet worm reportedly entered the computer network at a closed nuclear power plant located in Ohio, and disrupted its computer systems for over 5 hours.[12] Also, during the August 14, 2003 power blackout, the Blaster computer worm may have degraded the performance of several communications lines linking key data centers used by utility companies to manage the power grid.[13]

---

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

[9] Dan Eggan, May 1, 2003, *Center to Assess Terrorist Threat, Washington Post*, p. A10.

[10] Based on 2002 data submitted by federal agencies to the White House Office of Management and Budget, GAO noted, in testimony before the House Committee on Government Reform (GAO-03-564T, April 8, 2003), that all 24 agencies continue to have "significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption.", Christopher Lee, November 20, 2002, *Agencies Fail Cyber Test: Report Notes 'Significant Weaknesses' in Computer Security*, [http://www.washingtonpost.com/ac2/wp-dyn/A12321-2002Nov19?language=printer.]

[11] Symantec, February 2003, *Symantec Internet Security Threat Report*, p.48.

[12] Safety was not compromised because the Davis-Besse nuclear power plant at Lake Erie had been shut down since February 2003. This event indicated the potential for possible widespread disruption solely through transmission of malicious computer code. AP, September 4, 2003, *NRC Confirms Internet 'worm' Hit Ohio Plant*, Washington in Brief, *Washington Post*, p. A05.

[13] The exact cause of the blackout is still unknown, however, congestion caused by the Blaster worm delayed the exchange of critical power grid control data across the public telecommunications network, which could have hampered the operators' ability to prevent

(continued...)

Definition of Cyber Terrorism

It is first important to note that no single definition of the term "terrorism" has yet gained universal acceptance. Additionally, no single definition for the term "cyber terrorism" has been universally accepted. Also, labeling a computer attack as "cyber terrorism" is problematic, because it is often difficult to determine the intent, identity, or the political motivations of a computer attacker with any certainty until long after the event has occurred.

There are some emerging concepts, however, that may be combined to help build a working definition for cyber terrorism. Under 22USC, 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 term "international terrorism" means terrorism involving citizens or the territory of more than one country. The term "terrorist group" means any group practicing, or that has significant subgroups that practice, international terrorism.[14]

The National Infrastructure Protection Center (NIPC), now within DHS, defines cyber terrorism as "a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies."[15]

By combining the above concepts, "cyber terrorism" may also be defined as the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies. The definition may be extended by noting that DOD operations for information warfare[16] also include physical attacks on computer facilities and transmission lines.

Finally, other security experts reportedly believe that a computer attack may be defined as cyber terrorism if the effects are sufficiently destructive or disruptive to generate fear potentially comparable to that from a physical act of terrorism. Under this "severity of effects" view, computer attacks that are perhaps limited in scope, but

---

[13] (...continued)
the cascading effect of the blackout. Dan Verton, August 29, 2003, *Blaster Worm Linked to Severity of Blackout*, Computerworld, [http://www.computerworld.com/printthis/2003/0,4814,84510,00.html.]

[14] The US Government 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.]

[15] This definition comes from Ron Dick, 2002 Director of NIPC. Scott Berinato, March 15, 2002, *The Truth About Cyberterrorism*, CIO.

[16] DOD information warfare operations include the use of directed energy weapons that can deliver high-energy electromagnetic pulses to destroy computer circuits. Clay Wilson, March 14, 2003, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, CRS Report RL31787.

that lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence portions of the economy may also qualify as cyber terrorism.[17]

Why Computer Attacks are Successful

Networked computers with exposed vulnerabilities may be disrupted or taken over by an attacker. Computer hackers opportunistically scan the Internet looking for computer systems that do not have necessary or current software security patches installed, or that have improper computer configurations leaving them vulnerable to potential security exploits. Even computers with up-to-date software security patches installed may still be vulnerable to a type of attack known as a "zero-day exploit". This may occur if a computer hacker discovers a new vulnerability and launches a malicious attack program onto the Internet before a security patch can be created by the software vendor and made available to provide protection to software users. Should a terrorist group attempt to launch a coordinated attack against computers that manage the U.S. critical infrastructure, they may copy some of the tactics now commonly used by computer hacker groups to find computers with vulnerabilities and then systematically exploit those vulnerabilities (see Appendices A, B, and C).

Why Computer Vulnerabilities Persist

Vulnerabilities provide the entry points for a computer attack. Vulnerabilities persist largely as a result of poor security practices and procedures, inadequate training in computer security, and poor quality in software products.[18] For example, within some organizations, an important software security patch might not get scheduled for installation on computers until several weeks or months after the security patch is made available by the software product vendor.[19] Sometimes this delay may occur if an organization does not actively enforce its own security policy, or if the security function is under-staffed, or sometimes the security patch itself may disrupt the computer when installed, forcing the systems administrator to take additional time to adjust the computer configuration to accept the new patch. To avoid potential disruption of computer systems, sometimes a security patch is tested for compatibility on an isolated network before it is distributed for installation on other computers. As a result of delays such as these, the computer security patches that are actually installed and protecting computer systems in many organizations, at

---

[17] Dorothy Denning, November 2001, *Is Cyber War Next?*, Social Science Research Council, [http://www.ssrc.org/setp11/essays/denning.htm.]

[18] 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. SANS, April 15 2003, *The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities, 2003*, [http://www.sans.org/top20/].

[19] 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, August 25 2003, IT Managers Say They Are Being Worn Down by Wave of Attacks, Computeworld, Vol. 37, No. 34, P.1.

any point in time, may lag considerably behind the current cyber threat situation. Whenever delays for installing important security patches are allowed to persist in private organizations, in government agencies, or among home PC users, some computer vulnerabilities may remain open to possible attack for long periods of time.

Many security experts also emphasize that if systems administrators received proper training to adhere to strict rules for maintenance, such as installing published security patches in a timely manner or keeping their computer configurations secure, then computer security would greatly improve for the U.S. critical infrastructure.[20]

Commercial software vendors are often criticized for consistently releasing products with errors that create vulnerabilities.[21] Government observers have reportedly stated that approximately 80 percent of successful intrusions into federal computer systems can be attributed to software errors, or poor software quality.[22] Richard Clarke, former White house cyberspace advisor under the Clinton and Bush Administrations (until 2003), has reportedly said that many commercial software products have poorly written, or poorly configured security features.[23] There is currently no regulatory mechanism or legal liability if a software manufacturer sells a product that has design defects. Often the licensing agreement that accompanies the software product includes a disclaimer protecting the software vendor from all liability.

---

[20] According to security group Attrition.org, failure to keep software patches up to date resulted in 99 percent of 5,823 Web site defacements in 2003. Robert Lemos, 2003, *Software "fixes" routinely available but often ignored,* [http://news.com.com/2102-1017-251407.html].

[21] In September, 2003, Microsoft Corporation announced three new critical flaws in its latest Windows operating 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, September 15, 2003, *Attacks on New Windows Flaws Expected Soon,* Computerworld, Vol. 37, No. 37, p. 1.

[22] Johathan Krim, September 24, 2003, *Security Report Puts Blame on Microsoft,* Washingtonpost.com. Joshua Green, November 2002, *The Myth of Cyberterrorism,* The Washington Monthly, [http://www.washingtonmonthly.com/].

[23] 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 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, February 14, 2003, *White House issue 'National Strategy to Secure Cyberspace',* Network World Fusion, [http://www.nwfusion.com/news/2003/0214ntlstrategy.html.]

Many major software companies now contract for development of large portions of their software products in countries outside the United States.[24] Offshore outsourcing may give a programmer in a foreign country the chance to secretly insert a Trojan Horse or other malicious trapdoor into a new commercial software product. In 2003, GAO is reportedly beginning a review of DOD reliance on foreign software development to determine the adequacy of measures intended to reduce these related security risks in commercial software products purchased for military systems.

Possible Effects of Cyber Attack

A cyber attack has the potential to create economic damage that is far out of proportion to the cost of initiating the attack.[25] Security experts disagree about the damage that might result from a cyber attack,[26] and some have reportedly stated that U.S. infrastructure systems are resilient and could possibly recover easily from a cyber terrorism attack, thus avoiding any severe or catastrophic effects.

Lower Risk, but Less Drama. Tighter physical security measures now widely in place may actually encourage terrorists in the future to explore cyber terror as a form of attack that offers lower risk of detection to the attackers, with effects that could possibly cascade to disrupt other information systems throughout the critical infrastructure.[27] A successful cyber attack that targets vulnerable computers, causing them to malfunction, can result in corrupted flows of information that may disable other downstream businesses that have secure computer systems previously protected against the same cyber threat. For example, cyber attacks that secretly corrupt secure credit card transaction data at retail Internet sites, could possibly cause that corrupted data to spread into banking systems and could erode public confidence in the financial sector, or in other computer systems used for global commerce. Also, some

---

[24] Gartner Inc., a technology research organization, has estimated that by 2004, more than 80% of U.S. companies will have had high-level discussions about offshore outsourcing, and 40% will have completed a pilot program. Patrick Thibodeau, June 30, 2003, *Offshore's Rise is Relentless*, Computerworld, Vol. 37, No. 26, p.1.

[25] The most expensive natural disaster in U.S. history, Hurricane Andrew, is reported to have caused $25 billion dollars 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, March 3, 2003, *GAO Review of Weapon Systems Software*, Email communication, MillerC@gao.gov.

[26] Some of China's military journals speculate that cyber attacks could disable American financial markets. The dilemma for this kind of attack is that China is as dependent on the same financial markets as the United States, and could suffer even more from disruption. With other critical infrastructures, the amount of damage that can be done is, from a strategic viewpoint, trivial, while the costs of discovery for a nation state could be very great. These constraints, however, do not apply to non-state actors like Al Qaeda. Cyber attacks could potentially be a useful tool for non-state actors who reject the global market economy. James Lewis, December 2002, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, [http://www.csis.org/tech/0211_lewis.pdf.]

[27] CFR, April 4, 2003, *Terrorism: An Introduction*, [http://www.terrorismanswers.com/terrorism.]

security experts reportedly have stated that because technology continuously evolves, it is incorrect to think that future cyber attacks will always resemble the past annoyances we have experienced from Internet hackers.

However, other security observers disagree, stating that terrorist organizations might be reluctant to use the Internet itself to launch an attack. Some observers believe that terrorists will avoid launching a cyber attack because it would involve less immediate drama, and have a lower psychological impact than a traditional physical bombing attack. These observers believe that unless a computer attack 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. Unless a cyber terror event can be designed to attract as much media attention as a physical terror event, the Internet may be better utilized by terrorist organizations as a tool for surveillance and espionage, rather than for cyber terrorism.[28]

SCADA Systems. Supervisory Control And Data Acquisition (SCADA) systems are computer systems relied upon by most critical infrastructure organizations to automatically monitor and adjust switching, manufacturing, and other process control activities, based on feedback data gathered by sensors. Some experts believe that these systems may be vulnerable to cyber attack, and that their importance for controlling the critical infrastructure may make them an attractive target for cyber terrorists. SCADA systems once used only proprietary [29] computer software, and their operation was confined largely to isolated networks. However, an increasing number of industrial control systems now operate using Commercial-Off-The-Shelf (COTS) software, and more are being linked via the Internet directly into their corporate headquarters office systems.[30] Some observers believe that SCADA systems are inadequately protected against a cyber attack, and remain

---

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

[29] 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 (See Appendix A), 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. 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.

[30] The "Slammer" worm corrupted for 5 hours the computer systems at the closed Davis-Besse nuclear power plant located in Ohio. The worm bypassed firewall security, and highlighted possible security issues that may arise whenever plant networks and corporate networks are interconnected. The Davis-Besse corporate network was found to have multiple connections to the Internet that bypassed the plant firewall. Kevin Poulsen, August 19 2003, *Slammer Worm Crashed Ohio Nuke Plant Network*, Security Focus, [http://www.securityfocus.com/news/6767.]

vulnerable because many of the organizations that operate them have not paid proper attention to computer security needs.[31]

However, other observers disagree, suggesting that the critical infrastructure and SCADA systems are more robust and resilient than early theorists of cyber terror have stated, and that the infrastructure would likely recover rapidly from a cyber terrorism attack. They cite, for example, that in the larger context of economic activity, water system failures, power outages, air traffic disruptions, and other cyber-terror scenarios are routine events that do not always affect national security. System failure is a routine occurrence at the regional level, where service may often be denied to customers for hours or days. Highly skilled engineers and technical experts who understand the systems would, as always, work tirelessly to restore functions as quickly as possible. Cyber terrorists would need to attack multiple targets simultaneously for long periods of time, perhaps in coordination with more traditional physical terrorist attacks, to gradually create terror, achieve strategic goals, or to have any noticeable effects on national security.[32]

Several simulations have been conducted to determine the effects that an attempted cyber attack might have on U.S. defense systems and the critical infrastructure. In 1997, DOD conducted a mock cyber attack to test the ability of DOD systems to respond to protect the national information infrastructure. That exercise, called operation "Eligible Receiver 1997" revealed dangerous vulnerabilities in U.S. military information systems.[33] In October 2002, a subsequent mock cyber attack against DOD systems, titled "Eligible Receiver 2003", indicated a need for greater coordination between military and non-military organizations to deploy a rapid computer counter-attack, or pre-emptive attack.[34]

In July 2002, the U.S. Naval War College hosted a three-day seminar-style war game called "Digital Pearl Harbor". The objective was to develop a scenario for a coordinated, cross-industry, cyber terrorism event involving mock attacks by computer security experts against critical infrastructure systems in a simulation of state-sponsored cyber warfare attacks. The exercise concluded that a "Digital Pearl

---

[31] 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 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 cyber security. Sharon Gaudin, July 19, 2002, *Security Expter: U.S. Companies Unprepared for Cyber Terror*, Datamation, [http://itmanagement.earthweb.com/secu/article.php/1429851].

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

[33] Christopher Casteilli, 2002, *DOD and Thailand Run Classified 'Eligible Receiver' Info-War Exercise*, Defense Information and Electronics Report, Vol. 77, No. 44.

[34] January 9, 2003, Briefing on "Eligible Receiver 2003" by DOD staff for the Congressional Research Service.

Harbor" in the United States was only a small possibility. However, a survey of war game participants after the exercise indicated that 79 percent believed that a strategic cyber attack is likely within the next 2 years.[35]

The U.S. Naval War College simulation showed that cyber attacks directed against SCADA systems controlling the electric power grid were only able to cause disruption equivalent to a temporary power outage that consumers normally experience. Simulated attempts to cripple the telecommunications systems were determined to be unsuccessful because system redundancy would prevent damage from becoming too widespread. The computer systems that appeared to be most vulnerable to simulated cyber attacks were the Internet itself, and systems that are part of the financial infrastructure.[36]

Capabilities for Cyber Attack

Stealth and pre-operational surveillance are important characteristics known to precede a computer attack launched by hackers. Similar characteristics have also been described as a "hallmark" of some previous Al Qaeda physical terrorist attacks and bombings (see Appendices A and C).[37]

---

[35] The simulation involved more than 100 participants. Gartner, Inc., July, 2002, *Cyberattacks: The Results of the Gartner/U.S. Naval War College Simulation*, [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, August 23, 2002, *War College Calls Digital Pearl Harbor Doable*, Government Computer News, [http://www.gcn.com/vol1_no1/daily-updates/19792-1.html.]

[36] 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, October 10, 2003, *Expect terrorist attacks on Global Financial System*, [http://www.theregister.co.uk/content/55/33269.html]

[37] The success of the Vehicle Borne Improvised Explosive Devices (VBIEDs) used in the May 11, 2003 terrorist attacks in Riyadh, very likely depended on extensive advance surveillance of the multiple targets. Protective measures against such attacks rely largely on watching for signs of this pre-operational surveillance. Gary Harter, May 15, 2003, *Potential Indicators of Threats Involving VBIEDs*, Homeland Security Bulletin, Risk Assessment Division, Information Analysis Directorate, DHS.

Launching a coordinated or widespread attack against critical infrastructure computers may call for significant resources to develop the required set of technically sophisticated hacker tools, and to also conduct the necessary pre-operational surveillance. It has been estimated that advanced structured cyber attacks against multiple systems and networks, including target surveillance and creation and testing of new hacker tools, may require 2 to 4 years of preparation, while a complex coordinated cyber attack causing mass disruption against integrated, heterogeneous systems may require 6 to 10 years or preparation.[38]

Terrorist Organizations. A report by The Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School concluded that the barrier to entry for widespread and severe computer attacks is quite high and that terrorist groups currently lack the capability to mount a meaningful operation. The report also concluded that it is more likely that less severe computer attacks will be used in the future to supplement physical terrorist attacks.[39]

At a conference of terrorism experts held in Paris in May 2000, participants analyzed the decision-making processes of terrorist organizations, and concluded that information technology would most likely not be used to cause events of mass disruption. They stated that terrorist organizations would likely select their targets carefully and limit the effects of an attack.[40]

Some news sources have reported that Al Qaeda operatives are not currently involved with high-technology. Many captured computers contain files that are not encrypted, or that use encryption that is easily broken, and many of Al Qaeda's "codes" consist of simple word substitutions, or flowery Arabic phrases. However, Osama Bin Laden has reportedly has taken steps to improve organizational secrecy through more clever use of technology.[41]

Several experts have also observed that Al Qaeda and other terrorist organizations may begin to change their use of computer technology:

- seized computers belonging to Al Qaeda indicate its members are now becoming familiar with hacker tools that are freely available over the Internet; [42]

---

[38] Dorothy Denning, 2002, *Levels of Cyberterror Capability: Terrorists and the Internet*, presentation, [http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt]

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

[40] David Tucker, September, 2000, *The Future of Armed Resistance: Cyberterror? Mass Destruction?*, report on conference held at the University Pantheon-Assas, Paris, May 15-17, 2000, [http://www.nps.navy.mil/ctiw/files/substate_conflict_dynamics.pdf .]

[41] David Kaplan, June 2, 2003, *Playing Offense: The inside story of how U.S. terrorist hunters are going after Al Qaeda*, U.S. News & World Report, pp.19-29.

[42] Richard Clarke, April 2003, *Vulnerability: What are Al Qaeda's Capabilities?* PBS (continued...)

- as computer-literate youth increasingly join the ranks of terrorist groups, what may be considered radical today will become increasingly more mainstream in the future;
- a computer-literate leader may bring increased awareness of the advantages of an attack on information systems that are critical to an adversary, and will be more receptive to suggestions from other, newer computer-literate members;
- once a new tactic has won widespread media attention, it likely will motivate other rival groups to follow along the new pathway; [43] and,
- potentially serious computer attacks may be first developed and tested by terrorist groups using small, isolated laboratory networks, thus avoiding detection of any preparation before launching a widespread attack.[44]

Members of Al Qaeda and other terrorist groups have a record of using computer networks in planning terrorist acts. Evidence suggests that terrorists used the Internet to plan their operations for September 11, 2001. Mouhammed Atta, the leader of the attacks, made his air ticket reservations online, and Al Qaeda cells reportedly were using Internet-based telephone services to communicate with other cells overseas.[45] Khalid Shaikh Mohammed, mastermind of the attacks against the World Trade Center, reportedly used Internet chat software to communicate with at least two airline hijackers.[46] International terrorist groups, including Al Qaeda, are also known to use advances in technology such as optoelectronics (such as military night-vision devices), special communications equipment, GPS systems, and other electronic equipment, according to DHS officials. DHS Homeland Security Bulletins advise that many terrorists may now have access to very expensive high technology equipment.

Other news reports have indicated that some terrorist organizations are becoming increasingly familiar with stronger encryption. Ramzi Yousef, recently sentenced to life imprisonment for helping to bomb the World Trade Center, had

---

[42] (...continued)
Frontline: Cyberwar, [http://www.pbs.org].

[43] Jerrold M. Post, Kevin G. Ruby, and Eric D. Shaw, Summer 2000, From Car Bombs to Logic Bombs: The Growing Threat From Information Terrorism, Terrorism and Political Violence, Vol.12, No.2, pp.97-122.

[44] Networking technologies, such as the Internet, are advantageous for attackers who are geographically dispersed. Networking supports redundancy within an organization, and it suggests the use of swarming tactics, new weapons, and other new strategies for conducting conflict that show advantages over traditional government hierarchies. Inflexibility is a major disadvantage when a hierarchy confronts a networked organization. Networks blend offensive and defensive functions, while hierarchies struggle with allocating responsibility for either. John Arquilla, David Ronfeldt, 2001, *Networks and Netwars*, Rand, Santa Monica, California, p.285.

[45] Audrey Cronin, 2003, *Behind the Curve*, Globalization and International Terrorism, pre-publication draft.

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

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.[47]

The PBS television news program, Frontline, reported in April 2003 that a computer captured in Afghanistan, belonging to Al Qaeda, contained models of dams and computer programs that analyze them. The implication was that Al Qaeda may be using computer technology to aid in a future terrorist attack. It was not made clear whether a possible future attack might be done through the Internet or target the computer facilities that control the dams. Some observers also believe that terrorist groups that operate in post-industrial societies, such as Europe and the United States, may be more likely to consider and employ computer attack and cyber terrorism than groups operating in developing regions with limited technological penetration.

Terrorist-Sponsoring Nations. The U.S. Department of State lists seven designated state sponsors of terrorism in 2002: Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan.[48] These countries are identified as sponsors for funding, weapons, and other materials for planning and conducting operations by terrorist groups. Elements in Iran are believed by some observers to have close links with Al Qaeda, and North Korea has continued to sell weapons and high-technology items to other countries designated as state sponsors of terrorism. However, it should be pointed out that a study of trends in Internet attacks determined that countries on the Department of State list generated less than one percent of all reported cyber attacks directed against selected businesses in 2002.[49]

News sources have reported that, other than a few Web site defacements, there was no evidence that a computer attack was launched by Iraq or by terrorist organizations against United States military forces during Gulf War II.[50] The security research organization, C4I.org, reported that prior to the March 2003 deployment of U.S. troops, traffic increased from Web surfers in Iraq using search terms such as, "Computer warfare," "NASA computer network," and "airborne computer." Experts interpreted the increased Web traffic as an indication that Iraq's government was increasingly relying on the Internet for intelligence gathering.[51]

Other news sources have reported recent statements made by Major General Song Young-geun, head of the Defense Security Command of South Korea, claiming that North Korea may currently be training more than 100 new computer hackers per

---

[47] Ibid. p.109.

[48] U.S. Department of State, April 30, 2003, *2002 Patterns of Global Terrorism Report*.

[49] Riptech Internet Security Threat Report, *Attack Trends for Q1 and Q2 2002*, [http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf.] (Riptech has recently been purchased by Symantec, Inc.)

[50] Kim Zetter, May 2003, *Faux Cyberwar*, Computer Security, Vol.6, No.5, p.22.

[51] Brian McWilliams, May 22, 2003, *Iraq's Crash Course in Cyberwar*, Wired News, [http://www.wired.com/news/print/0,1294,58901,00.html].

year.[52] Pentagon and State Department officials reportedly are unable to confirm the claims made by South Korea, and defense experts reportedly believe that North Korea is incapable of seriously disrupting U.S. military computer systems. Also, Department of State officials have reportedly said that North Korea is not known to have sponsored any terrorist acts since 1987. However, computer programmers from the Pyongyang Informatics Center in North Korea have done contract work to develop software for local governments and businesses in Japan and South Korea. And other security experts reportedly believe that North Korea may have also developed a considerable capability for cyber warfare, partly in response to South Korea's admitted build up of 177 computer training centers and its expanding defense budget targeted at projects to prepare for information warfare.[53]

Possible Links Between Hackers and Terrorists

Hacker groups are numerous, and have differing levels of technical skill. Membership in highly-skilled hacker groups may be exclusive, and limited only to individuals who develop and share their own closely-guarded set of sophisticated hacker tools. These exclusive hacker groups are more likely to not seek attention because secrecy allows them to be more effective.

Some hacker groups may be globally dispersed, with political interests that are supra-national, or based on religion or other socio-political ideologies. Other groups may be motivated by profit, or linked to organized crime, and may be willing to sell their computer skills to a sponsor, such as a nation state or a terrorist group, regardless of the political interests involved. For instance, it has been reported that the Indian separatist group, Harkat-ul-Ansar, attempted to purchase military software from hackers in late 1998. In March 2000, it was reported that the Aum Shinrikyo cult organization had contracted to write software for up to 80 Japanese companies, and 10 government agencies, including Japan's Metropolitan police department; however, there were no reported computer attacks related to these contracts.[54]

Linkages between hackers, terrorists, and terrorist-sponsoring nations may be difficult to confirm, but cyber terror activity may possibly be detected through careful monitoring of network chat areas where hackers sometimes meet anonymously to exchange information. The Defense Advanced Research Projects Agency (DARPA) has conducted research and development for systems, such as the former Terrorism

---

[52] The civilian population of North Korea is reported to have a sparse number of computers, with only a few locations offering connections to the Internet, while South Korea is one of the most densely-wired countries in the world, with 70 percent of all households having broadband Internet access. During the recent global attack involving the "Slammer" computer worm, many Internet service providers in North Korea were severely affected. Miami Herald Online, May 16, 2003, *North Korea May be Training Hackers*, [http://www.miami.com/mld/miamiherald/news/world/5877291.htm].

[53] Brian McWilliams, June 2, 2003, *North Korea's School for Hackers*, Wired News.com, [http://www.wired.com/news/conflict/0,2100,59043,00.html].

[54] Dorothy Denning, August 24, 2000, *Cyber terrorism*, [http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc].

Information Awareness Program,[55] that are intended to help investigators discover covert linkages among people, places, things, and events related to possible terrorist activity (see below for privacy issues).

Issues for Congress

Issues linked to a DOD Response to Cyber Terrorism

In February 2003, the administration published a report titled, the "National Strategy to Secure Cyberspace", that makes clear that the U.S. government reserves the right to respond "in an appropriate manner" if the United States comes under computer attack. This response could involve the use of U.S. cyber weapons, or malicious code designed to attack and disrupt the targeted computer systems of an adversary.

Guidance for DOD. The Bush administration announced plans, in February, 2003, to develop national-level guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems.[56] However, any U.S. response against a cyber attack must be carefully weighed to avoid mistakes in retaliation, or other possible unintended outcomes.

A potential issue for Congress is that any response intended by U.S. forces as retaliation may be labeled by others as an unprovoked first strike against the targeted terrorist group. Similarly, any U.S. attempt to suddenly or greatly increase surveillance via use of computer programs may be labeled as an unprovoked attack against a terrorist group. Options for a cyber response from the United States may be limited because there will likely be difficulty in determining, with a high degree of certainty, or in a timely manner, if a terrorist group is responsible for a cyber attack against the United States. For example, any identifiable source of a computer attack might have previously had its own computers taken over by an intruder. Thus, a terrorist group could possibly be set up by others to appear as the guilty cyber attacker in order to draw attention away from the actual attacker who may be located elsewhere.

---

[55] Funding for the controversial Terrorism Information Awareness program has ended for 2004. The prototype system was formerly housed within the DARPA Information Awareness Office. Several related data mining research and development programs, now under different agencies, are designed to provide better advance information about terrorist planning and preparation activities to prevent future international terrorist attacks against the United States at home or abroad. A goal of data mining is to treat worldwide distributed database information as if it were housed within one centralized database. *Report to Congress Regarding the Terrorism Information Awareness Program*, Executive Summary, May 20 2003, p.1.

[56] The guidance, known as National Security Presidential Directive 16, was signed in July 2002, and is intended to clarify circumstances under which an information warfare attack by DOD would be justified, and who has authority to launch a computer attack.

U.S. Use of Cyber Weapons. If the United States should officially choose to use DOD cyber weapons to retaliate against a terrorist group, would that possibly encourage others to then start launching cyber attacks against the United States? If a terrorist group should subsequently copy, or reverse-engineer a destructive U.S. military computer attack program, would they use it against other countries that are U.S. allies, or even turn it back against civilian computer systems in the United States?[57]

The use of cyber weapons, if the effects are widespread and severe, could arguably exceed the customary rules of military conflict, also known as the international laws of war.[58] The resulting effects of offensive cyber weapons for information warfare operations may be difficult to limit or control. If a computer attack program is targeted against terrorist groups or enemy military computer systems, there is a possibility that the malicious code might inadvertently spread throughout the Internet to severely affect or shut down critical infrastructure systems in other non-combatant countries, including perhaps computers operated by U.S. friends and allies, or other U.S. interests. Critical civilian computer systems within the country hosting the terrorist group may also be adversely affected by a DOD cyber attack against the terrorists' computers.

In a meeting held in January 2003, at the Massachusetts Institute of Technology, White House officials sought input from experts outside government on guidelines for U.S. use of cyber weapons. Officials have stated they are proceeding cautiously, because a U.S. cyber attack against terrorist groups or other adversaries could have serious cascading effects, perhaps causing major disruption to civilian systems in addition to the intended computer targets.[59]

Privacy

Another potential issue for Congress concerns how to balance the need for terrorism awareness against the need to protect individual privacy. A factor limiting the ability to analyze the cyber capabilities of terrorist groups is a lack of data related to computer activity that can be traced back to those groups. A terrorist group that is currently lacking the technical skills needed to scan for vulnerabilities and launch a computer-based attack may possibly gain access to additional resources through

---

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

[58] 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. For example, innocent civilians are protected during war under the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to be Excessively Injurious or to have Indiscriminate Effects. 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, vol. 15, no. 1, p.25-36.

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

forming a link with hacker criminals, or with one of several terrorist-sponsoring nation states. Data mining programs such as the former Terrorism Information Awareness program, and the new Terrorist Threat Information Center (TTIC) are intended to help uncover these linkages. However, concerns raised about possible loss of individual privacy through investigation of domestic databases has resulted in restrictions on development of automated tools for analysis of information.

Terrorism Information Awareness Program. Funding has ended for the Terrorism Information Awareness (TIA) program for 2004, and the Information Awareness Office, a branch of DARPA, is now disbanded.[60] The TIA data mining program was intended to sift through vast quantities of citizens' personal data, such as credit card transactions and travel bookings, to identify possible terrorist activity to provide better advance information about terrorist planning and preparation activities to prevent future international terrorist attacks against the United States at home or abroad.

However, the TIA program and other similar proposals for domestic surveillance raised privacy concerns from lawmakers, advocacy groups, and the media. Some privacy advocates have objected to the possibility that information gathered through domestic surveillance may be viewed by unauthorized users, or even misused by authorized users. Congress has moved to restrict or eliminate funding for the TIA program under S. 1382 and H.R. 2658.

S. 1382, titled the Defense Appropriations Act of 2004, and introduced on 7/9/2003 by Senator Ted Stevens, restricts funding and deployment of the TIA Program. Section 8120 part (a) limits use of funds for research and development of the TIA Program, stating that "no funds appropriated or otherwise made available to the Department of Defense, whether to an element of the Defense Advanced Research Projects Agency or any other element, or to any other department, agency, or element of the Federal Government, may be obligated or expended on research and development on the Terrorism Information Awareness program." Section 8120 part (b) limits deployment of TIA systems, stating that no department or agency of the Federal Government may deploy or implement any component of TIA, until the Secretary of Defense notifies Congress about the intended deployment and has received authorization from Congress.

H.R. 2658, titled Defense Appropriations FY2004, was introduced on 7/2/2003 by Representative Jerry Lewis, and requires specific authorization by law from Congress for the deployment or implementation of any component of the TIA program, if research and development facilitate such deployment or implementation. In September, under section 8131, and in House Report 108-283, House and Senate conferees agreed to end funding for TIA for 2004, and to disband the Information Awareness Office (IAO) of DARPA. However, other

[60] House and Senate conferees voted on September 24 to end funding for TIA through 2004. Steven M. Cherry, September 29, 2003, *Controversial Pentagon Program Scuttled, But Its Work Will Live On*, IEEE Spectrum online, [http://www.spectrum.ieee.org].

DOD programs for foreign counterintelligence under the CIA, FBI and NSA, and several other research programs formerly within the IAO are continued.[61]

Other Search Technologies. The Department of Defense is currently reviewing the capabilities of other data mining products using technology that may reduce domestic privacy concerns raised by TIA. For example, Systems Research and Development, a technology firm based in Las Vegas, has been tasked by the CIA and other agencies to develop a new database search product called "Anonymous Entity Resolution." The technology used in this product can help investigators determine whether a terrorist suspect appears in two separate databases, without revealing any private individual information. The product uses encryption to ensure that even if the scrambled records are intercepted, no private information can be extracted. Thus, terrorism watch lists and corporate databases could be securely compared online, without revealing private information.[62]

The Florida police department has, since 2001, operated a counter terrorism system called the Multistate Anti-Terrorism Information Exchange, or "Matrix", that helps investigators find patterns among people and events by combining police records with commercially available information about most U.S. adults. Matrix includes information that has always been available to investigators, but adds extraordinary processing speed. The Justice Department has provided $4 million to expand the Matrix program nationally. DHS has pledged $8 million to assist with the national expansion, and has also announced plans to launch a pilot data-sharing network that will include Virginia, Maryland, Pennsylvania, and New York.[63]

---

[61] The eight programs formerly within the now disbanded IAO, but still remaining under DARPA are: Bio-Event Advanced Leading Indicator Recognition Technology ($6.3M); Rapid Analytical Wargaming ($7.5M); Wargaming the Asymmetric Environment ($8.2M); and five projects to translate and analyze spoken and written natural languages - TIDES, EARS, and GALE ($46.3M), and Babylon and Symphony ($10.9M). Related research will also continue for a counterintelligence program known as the National Foreign Intelligence Program, managed jointly by the CIA, FBI and NSA. The budget for the NFIP is classified. Steven M. Cherry, September 29, 2003, *Controversial Pentagon Program Scuttled, But Its Work Will Live On*, IEEE Spectrum online, [http://www.spectrum.ieee.org].

[62] Pentagon sources familiar with the "Anonymous Entity Resolution" technology have indicated that it may alleviate some of the issues associated with privacy protection. The product uses "entity-resolution techniques" to scramble data for security reasons. The software sifts through data such as names, phone numbers, addresses and information from employers to identify individuals listed under different names in separate databases. The software can find information by comparing records in multiple databases, however the information is scrambled using a "one-way hash function," which converts a record to a character string that serves as a unique identifier like a fingerprint. Persons being investigated remain anonymous, and agents can isolate particular records without examining any other personal information. A record that has been one-way hashed cannot be "un-hashed" to reveal information contained in the original record. Steve Mollman, March 11, 2003, *Betting on Private Data Search*, Wired.com.

[63] Robert O'Harrow, August 6 2003, *U.S. Backs Florida's New Counterterrorism Database*, *Washington Post*, p. A01.

For more information about TIA, data mining technology, and other related privacy issues, see CRS Reports RL31786, RL31730, RL31798, or RL31846.

The Roles of Government, Industry, and Home Users

National Director for Cyber Security. A potential issue for Congress is whether the new national director for cyber security is a position senior enough within DHS to elevate concerns about cyber security to an appropriate level, relative to other concerns about physical security.[64] Early plans for naming the new cyber security director were seen as closely guarded by the administration, causing some industry observers to express concern that cyber security may be losing visibility within the administration.[65] In September 2003, DHS formally announced Amit Yoran as new director of its cyber security division, with responsibility for implementing recommendations to improve national cyber security.

National Strategy to Secure Cyberspace. Another potential issue is whether the National Strategy to Secure Cyberspace should rely on voluntary action on the part of private firms, home users, universities, and government agencies to keep their networks secure, or whether there may be a need for possible regulation to ensure best security practices. Some security experts believe that public response has been slow to improve computer security despite warnings about possible cyber terrorism, partly because there are no regulations currently imposed by the National Strategy to Secure Cyberspace.[66] Others in the technology industry, however, believe that regulation would interfere with innovation and possibly harm U.S. competitiveness.

Commercial Software Vulnerabilities. Another issue is whether software product vendors should be required to create higher quality software products that are more secure and that need fewer patches. Software vendors may increase the level of

---

[64] The DHS cybersecurity center will have five primary roles: conducting cybersecurity research; developing performance standards; fostering public-private sector communication; supporting the DHS information analysis and infrastructure protection directorate; and working with the National Science Foundation on educational programs. CongressDailyAM, May 15, 2003.

[65] The Department of Homeland Security has selected Amit Yoran, formerly vice president for Managed Security Services at Symantec Corporation, to lead the agency's cyber-security division, Caron Carlson, September 15, 2003, *Feds Tap Cyber Security Chief*, Computer Cops, [http://computercops.biz/article3138.html.]

[66] 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 percent 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 dollars spent on IT projects between 1977 and 2000 in preparation for the year 2000 (Y2K) changeover, now viewed by some as a non-event. Sources reported that some board-level executives stated that the Y2K problem was overblown and over funded then, and as a result, they are now much more cautious about future spending for any new, massive IT initiatives. Gary H. Anthes and Thomas Hoffman, May 12, 2003, *Tarnished Image*, Computerworld, Vol. 37, No. 19, p. 37.

security for their products by rethinking the design, or by adding more test procedures during product development. However, some vendors reportedly have said that their customers may not be willing to pay the costs for additional security, and that additional testing will slow the innovation process and possibly reduce U.S. competitiveness in the global software market.[67]

Awareness and Education. Should computer security training be offered to all computer users to keep them aware of constantly changing computer security threats, and to encourage them to follow proper security procedures to protect against possible cyber attack? One type of cyber attack, known as "Denial of Service", has been known to occur when thousands of individual PCs are secretly taken over by attack programs, and then directed to collectively overpower and disable one or more targeted computers located elsewhere on the Internet. Many of the PCs taken over by hackers may belong to individual home users who have not had computer security training, but who may currently feel no motivation to voluntarily participate in a training program.

Coordination to Protect Against Cyber Terrorism

Coordination between the private sector and government requires mutual confidence about any information they exchange on computer security vulnerabilities.[68] To be most effective, cyber security requires sharing of information about threats, vulnerabilities, and exploits. The private sector wants information from the government on specific threats which the government may currently consider classified. The government wants specific information from private industry about vulnerabilities and incidents which companies say they want to protect to avoid publicity and to guard trade secrets. A recent GAO survey of local government officials also found that there was currently no process for effectively sharing state and city information with federal agencies. The GAO study recommended that DHS strengthen information sharing by incorporating states and cities into its "enterprise architecture" planning process.[69]

Information Sharing. A potential issue for Congress is whether to protect from public disclosure through FOIA any vulnerability information that is voluntarily shared between private companies and state, local, and federal government. DHS, in a recent notice of proposed rule making (see [http://edocket.access.gpo.gov/2003/03-9126.htm]), indicated that technology and telecommunications companies should voluntarily submit information to DHS whenever a security vulnerability is discovered in one of their products. DHS

---

[67] Building in more security adds to the cost of a software product. Now that software features are similar across brands, software vendors have indicated that their customers, including federal government agencies, often make purchases based largely on product price. NSA, 2001, *Conference on Software Product Security Features*, Information Assurance Technical Information Framework Forum,, Laurel, Maryland.

[68] John Moteff, August 7, 2003, *Critical Infrastructures: Background, Policy and Implementation*, p. CRS-28.

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

proposed that this critical infrastructure information should be protected from unauthorized disclosure. However, the proposal is controversial because that protection possibly may not extend to requests for disclosure under FOIA,[70] and also, conversely, because media and public advocacy groups are concerned that industries will use the process to shield information that might otherwise be available through FOIA.

International Issues. Should the U.S. find effective ways to encourage more international cooperation during attempts to trace and identify a cyber attacker? As yet, no evidence has been published to confirm that a computer attack has been launched against U.S. critical infrastructure targets for terrorist purposes,[71] but the problem may be masked because there is currently no reliable way to determine the origin of a computer attack.[72] Attackers can hide details of their true location by hopping from one computer system to another, sometimes taking a path that connects networks and computers in many different countries. Pursuit may involve a trace back through networks requiring the cooperation of many Internet Service Providers located in several different nations. 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.[73]

Another potential issue is whether U.S. national security may be threatened by using commercial software products developed in foreign countries.[74] Commercial software development is increasingly outsourced to foreign countries, raising questions about possible imbedded vulnerabilities created by foreign programmers who may sympathize with terrorist objectives. A recent study by Gartner Inc., a technology research organization, predicts that by 2004, more than 80 percent of U.S. companies will consider outsourcing critical IT services, including software

---

[70] Shawn P. McCarthy, 2003, *HDS Should fix a Big Weakness: Spoofing*, Vol. 22, no.10, p.30, [http://www.gcn.com].

[71] In May 1998, U.S. intelligence officials told reporters in a briefing that an ethnic group called the Tamil Tigers, a guerrilla group also labeled as a terrorist organization, attempted to swamp Sri Lankan embassies with electronic mail. Anthony Townsend, May 5, 1998, *First Cyberterrorist Attack Reported by U.S.*, Reuters.

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

[73] In Argentina, a group calling themselves the X-Team, hacked into the web site 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 web sites. The group on trial was declared not guilty of breaking into the web site. Paul Hillbeck, *Argentine judge rules in favor of computer hackers*, February 5, 2002, [http://www.siliconvalley.com/ mld/siliconvalley/news/editorial/3070194.htm].

[74] In 2000, news sources reported that the Defense Agency of Japan halted the introduction of a new computer system after discovering that some of the software had been developed by members of the Aum Shinrikyo cult, which was responsible for the fatal 1995 Tokyo subway gas attack. The Defense Agency was one of 90 government agencies and industry firms that had ordered software produced by the cult. Richard Power, 2000, *Current & Future Danger: A CSI Primer on Computer Crime and Information Warfare*, Computer Security Institute.

development. Corporations justify their actions by saying that global economic competition makes outsourcing of IT projects overseas a business necessity. Oracle, a major database software vendor and a supplier to U.S. intelligence agencies, has in the past contracted for software development in India and China. Terrorist networks are known to exist in other countries located in Southeast Asia where some contract work has been outsourced, such as Malaysia and Indonesia. Other possible recipients of outsourced projects are countries such as Israel, India, Pakistan, Russia and China.[75]

Options for Congress

Privacy

Congress may wish to consider whether more research should be encouraged into database search technologies that provide more protection for individual privacy while helping to detect terrorist activities. Pre-operative surveillance and anonymous meetings via the Internet now characterize the early planning stages of many cyber attacks launched by hackers. A cyber terrorist attack may possibly involve similar characteristics during the planning stage that may be detectable before the attack can be launched.

The Roles of Government, Industry, and Home Users

Another issue concerns setting standards to improve national computer security. Some observers have reportedly stated that the annual Computer Security Institute (CSI) computer security survey, which is often relied upon as a measure of current trends in computer security threats and vulnerabilities, is actually limited in scope and may possibly contain statistical bias.[76] This has led to suggestions for an analysis of costs and benefits for setting standards to improve computer security, aiming towards a more carefully designed and statistically reliable analysis of threats, risks, and the costs and benefits associated with alternate policies to improve cyber security by indicating which security practices are most effective and efficient.

Another issue concerns the extent to which public officials and industry managers should be held responsible for their performance in ensuring cyber security. Some observers reportedly have indicated that the National Strategy to Secure Cyberspace currently may not present a clear link between security objectives and the incentives required to help achieve those objectives.

---

[75] Dan Verton, May 5, 2003, *Offshore Coding Work Raises Security Concerns*, Computerworld, Vol.37, No.18, p. 1.

[76] Respondents to the CSI survey of computer security issues are generally limited to CSI members. Recently, CSI has conceded weaknesses in its analytical approach and has suggested that its survey of computer security vulnerabilities and incidents may be more illustrative than systematic. Bruce Berkowitz and Robert W. Hahn, Spring 2003, *Cybersecurity: Who's Watching the Store?*, Issues in Science and Technology.

There are suggestions to examine ways to provide incentives that motivate the software industry to improve the security and quality of their products before they are released for purchase.[77] One option mentioned would include, as part of the requirement for the purchase of civilian agency software, certification under the "Common Criteria"[78] testing program, as is now required for the purchase of military software. However, industry observers point out that the certification process is lengthy, and may interfere with innovation and competitiveness.

Coordination to Protect Against Cyber Terrorism

Information Sharing. Another issue is whether voluntary information should be shielded from disclosure through Freedom of Information Act requests. Proponents argue that information about computer security threats and vulnerabilities, if shared more effectively, could help both industry and government systematically reduce cyber security vulnerabilities, and identify attempted cyber terrorism activity. However, many firms are reluctant to share this important information with government agencies because of the possibility of having competitors become aware of a company's security vulnerabilities.

S. 609 - This legislation proposes to reduce the number of categories for exemptions to FOIA now proposed under Section 214 of the Homeland Security Act, because of concerns about limitations to freedom of the press. The bill was referred to Committee on the Judiciary on March 12, 2003.

Education and Incentives. Many of the same vulnerabilities that affect government and corporate computers, requiring systems administrators to install software patches, also affect computers belonging to millions of home PC users.[79] Congress may wish to examine ways to provide education, such as public awareness

---

[77] In the wake of widespread attacks by Internet worms, Microsoft is weighing options to get more users to secure their computers, including automatically applying security patches to PCs remotely. Joris Evers, August 22, 2003, Microsoft Ponders Automatic Patching, NetworkWorldFusion, [http://www.nwfusion.com/news/2003/0822mspatch.html].

[78] 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 organization that works in parallel to similar 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, however, the administration has stated that the government will undertake a review of the program in 2003 to "possibly extend" it as a requirement for civilian agencies. Ellen Messmer, February 14, 2003, *White House issue 'National Strategy to Secure Cyberspace'*, Network World Fusion, [http://www.nwfusion.com/news/2003/0214ntlstrategy.html].

[79] A spokesperson for the Computer Emergency Response Team at Carnegie Mellon has reportedly stated that most people may not yet realize that anti-virus software and a firewall are no longer enough to protect computers anymore. Charles Duhigg, August 28 2003, Fight Against Viruses May Move to Servers, *Washington Post*, p.E01.

messages about computer security, or provide other incentives to encourage home PC users to follow the best security practices.

Legislative Activity

The Cyber Security Research and Development Act (P.L. 107-305), authorized $903 million over five years for new research and training programs by the National Science Foundation and NIST to prevent and respond to terrorist attacks on private and government computers. The House Science Committee also held a hearing on May 14, 2003 on Cybersecurity Research and Development, with testimony by the DHS Under Secretary for Science and Technology. A $5 million budget allocation is currently set aside for Information Technology R&D.

The Subcommittee on Cybersecurity, Science, and Research & Development of the House Select Committee on Homeland Security also held a series of hearings on cyber security issues during the summer of 2003. The series was intended to (1) raise awareness among members of Congress about cyber security risks, (2) examine the views of security experts on the state of security for the critical infrastructure, (3) present the views of industry experts on how DHS might best help resolve cyber security issues, and (4) provide an opportunity for DHS officials to respond to questions raised in the preceding three hearings. On October 1, 2003, the Subcommittee also held an executive session oversight hearing titled, "Security of Industrial Control Systems in Our Nation's Critical Infrastructure" with testimony provided by government agencies and by experts on industrial computer systems.

Following the September 11, 2001 attacks, the Federal Information Security Management Act (FISMA) of 2002 was enacted giving responsibility for setting security standards for civilian federal agency computer systems to the Office of Management and Budget (OMB).[80] Responsibility for security standards for national defense systems remains primarily with DOD and NSA.

The following bills identify recent legislative activity that is related to prevention of cyber terrorism, or related to collection of information on possible terrorist activities.

1. **S. 6** - proposes that information about vulnerabilities and threats to the critical infrastructure that is furnished voluntarily to the DHS shall not be made available either to the public or other federal agencies under the Freedom of Information Act. This bill was referred to Committee on the Judiciary on January 7, 2003.

---

[80] Under FISMA, the Director of OMB (1) oversees the implementation of information security policies for civilian federal agencies, (2) requires agencies to identify and provide information security protection appropriate for the level of risk and magnitude of harm resulting from possible destruction of information or systems, and (3) coordinates the development of security standards and guidelines developed between NIST, NSA, and other agencies to assure they are complementary with standards and guidelines developed for national security systems. See 44 U.S.C., Section 3543 (a).

2. **S. 187** - proposes to eliminate IT vulnerabilities in the federal government to protect against cyber attacks and possible cyber terror. The National Cyber Security Leadership Act of 2003, if passed, will require the Chief Information Officer of each Federal agency to report annually to the Director of OMB to: (1) identify the significant vulnerabilities of the information technology of such agency; (2) establish performance goals for eliminating such vulnerabilities; (3) procure or develop tools to identify and eliminate those vulnerabilities in order to achieve such performance goals; (4) train personnel in the utilization of those tools; (5) test the agency's IT to determine the extent of its compliance with the performance goals; and (6) develop and implement a plan to eliminate significant vulnerabilities in order to achieve compliance. The bill was referred to the Committee on Government Affairs on January 16, 2003.

Appendix A - Planning a Computer Attack

There are five basic steps traditionally used by computer hackers to gain unauthorized access, and subsequently take over computer systems. These five steps may be used to plan a computer attack for purposes of cyber crime or cyber espionage, and may also be employed for purposes of cyber terror. The steps are frequently automated through use of special hacker tools that are freely available to anyone via the Internet.[81] Highly-skilled hackers use automated tools that are also highly sophisticated, and their effects are initially much more difficult for computer security staff and technology to detect. These sophisticated hacker tools are usually shared only among an exclusive group of other highly-skilled hacker associates. The hacker tactics described in this report are also explained in detail in many existing books that list possible defenses against computer attack, including "Counter Hack" by Ed Skoudis, 2002.

- Step 1. Reconnaissance
  In this first step, hackers employ extensive pre-operative surveillance to find out detailed information about an organization that will help them later gain unauthorized access to computer systems. The most common method is social engineering, or tricking an employee into revealing sensitive information (such as a telephone number or a password). Other methods include dumpster diving, or rifling through an organization's trash to find sensitive information (such as floppy disks or important documents that have not been shredded). This step can be automated if the attacker installs on an office computer a virus, worm, or "Spyware" program that performs surveillance and then transmits useful information, such as passwords, back to the attacker. "Spyware" is a form of malicious code that is quietly installed on a computer without user knowledge when a user visits a malicious web site. It may remain undetected by firewalls or current anti-virus security products[82] while monitoring keystrokes to record web activity or collect snapshots of screen displays and other restricted information for transmission back to an unknown third party.

- Step 2.Scanning
  Once in possession of special restricted information, or a few critical phone numbers, an attacker performs additional surveillance by scanning an organization's computer software and network configuration to find possible entry points. This process goes slowly, sometimes lasting months, as the attacker looks for several vulnerable openings into a system.[83]

---

[81] Using these five basic steps, often supplemented with automated intrusion tools, attackers have successfully taken over computer systems and remained undetected for long periods of time. Ed Skoudis, *Counter Hack*, Prentice Hall, New Jersey, 2002.

[82] For more about Spyware, see Spywareinfo at [http://www.spywareinfo.com/].

[83] An attacker may use an automatic "War Dialing" tool that dials thousands of telephone numbers, looking for modems connected to a computer. If a computer modem answers when the War Dialer calls, the attacker may have located a way to enter an organization's

(continued...)

- Step 3.Gaining Access
  Once the attacker has developed an inventory of software and configuration vulnerabilities on a target network, he or she may quietly take over a system and network by using a stolen password to create a phony account, or by exploiting a vulnerability that allows them to install a malicious Trojan Horse, or automatic "bot" that will await further commands sent through the Internet.

- Step 4: Maintaining access
  Once an attacker has gained unauthorized access, he or she may secretly install extra malicious programs that allow them to return as often as they wish. These programs, known as "Root Kits" or "Back Doors", run unnoticed and can allow an attacker to secretly access a network at will. If the attacker can gain all the special privileges of a system administrator, then the computer or network has been completely taken over, and is "owned" by the attacker. Sometimes the attacker will reconfigure a computer system, or install software patches to close the previous security vulnerabilities just to keep other hackers out.

- Step 5: Covering Tracks
  Sophisticated attackers desire quiet, unimpeded access to the computer systems and data they take over. They must stay hidden to maintain control and gather more intelligence, or to refine preparations to maximize damage. The "Root Kit" or "Trojan Horse" programs often allow the attacker to modify the log files of the computer system, or to create hidden files to help avoid detection by the legitimate system administrator. Security systems may not detect the unauthorized activities of a careful intruder for a long period of time.[84]

---

[83] (...continued)
network and bypass firewall security. A newer way of scanning for vulnerabilities is called "War Driving", where hackers drive randomly through a neighborhood trying to detect signals from business or home wireless networks. Once a network is detected, the hacker may park nearby and attempt to log on to gain free, unauthorized access. Kevin Poulsen, April 12 2001, *War Driving by the Bay*, Securityfocus.com, [http://www.securityfocus.com/news/192].

[84] New "antiforensics tools" are now available on the Internet that allow hackers to more effectively hide their actions, and thus defeat more investigators who search for technical evidence of computer intrusions. Anne Saita, May 2003, *Antiforensics: The Looming Arms Race*, Information Security, Vol. 6, No. 5, p.13.

Appendix B - Technology of Malicious Code

Technology constantly evolves, and new security vulnerabilities are discovered regularly by software vendors, by security organizations, by individual researchers, and often by computer hacker groups.[85] Security organizations, such as the Computer Emergency Response Team (CERT/CC) located at Carnegie Mellon, publish security advisories, including information about new software patches, usually before computer hacker groups can take advantage of newly discovered computer security vulnerabilities for purposes of cyber crime or cyber espionage. However, despite numerous alerts, the number of reported unauthorized computer intrusions has increased every year, with a 56 percent increase reported between 2001 and 2002.[86]

Currently, attacks are enabled by "infecting" a computer with a malicious payload program that corrupts data, performs surveillance, or that receives commands through the Internet to paralyze or deny service to a targeted computer. A computer may become "infected" if a computer user mistakenly downloads and installs a malicious program, or mistakenly opens an infected email attachment. Other malicious programs, known as "worms", may actively and rapidly seek out other computers on the Internet having a specific non-patched vulnerability, and automatically install themselves without any action required on the part of the victim.[87]

A virus is one form of malicious program that often immediately corrupts data or causes a malfunction. A Trojan Horse is another form of malicious program that

---

[85] In September 2003, DHS warned U.S. industry and the federal government to expect potentially significant attacks to emerge against Internet operations, similar to the recent Blaster worm exploit, because of newly discovered critical flaws in Windows software that were announced by Microsoft Corporation. Jaikumar Vijayan, September 15, 2003, *Attacks on New Windows Flaws Expected Soon*, Computerworld, Vol. 37, No. 37, p. 1.

[86] A single reported computer security incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time. CERT estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated, or there were no indications of penetration or attack, or (2) the organization was reluctant to publicly admit to being a victim of a computer security breach. CERT,2003, *CERT/CC Statistics 1988-2002*, 2003, April 15, [http://www.cert.org/stats/cert_stats.html#incidents.] CERT, 2003, *CERT/CC Statistics*, 2003, [http://www.cert.org/stats/cert_stats.html.]

[87] MARC Commuter and CSX freight rail service experienced cancellations and delays on August 21, 2003, because of a virus that disabled the computer systems at the CSX railway Jacksonville, Florida headquarters. The recent "Blaster" worm attacked more than 500,000 computers worldwide within one week. The "Blaster" attack was quickly followed the next week by another worm that spread worldwide, called "Welchia", which installed itself on computers by taking advantage of the same vulnerability used by Blaster. Brian Krebs, August 18 2003, *'Good' Worm Fixes Infected Computers*, Washingtonpost.com. The "Welchia" worm also disrupted the highly secure Navy Marine Corps Intranet (NMCI) during the week of August 11, by flooding it with unwanted traffic. This was the first time in the history of the highly secure network that it was disrupted by an outside cyber attack. Diane Frank, August 25 2003, Attack of the Worms: Feds Get Wake-Up Call, Federal Computer Week, Vol 17, No. 29, p.8.

quietly and secretly displaces the functions of an existing trusted program on the computer. An attack program, once installed, may quietly "listen" for a special command sent through the Internet from a remote source, instructing it to begin activation of malicious program instructions. Another type of malicious program, known as "spyware", has a surveillance or espionage capability that enables it to secretly record and automatically transmit keystrokes and other information (including passwords) back to a remote attacker.[88] Other types of malicious code may combine some or all of the characteristics of viruses, worms, Trojan Horses, or spyware along with the ability to randomly change the electronic appearance (polymorphism) of the resulting attack code. This ability to change makes many of the newer viruses, worms, and Trojan Horses very difficult for most anti-virus security products to detect.[89]

Malicious programs attack by disrupting normal computer functions, or by opening a back door for a remote attacker to take control of the computer. Sometimes an attacker can quietly take full control of a computer with the owner remaining unaware that his or her machine is compromised. An attack can either immediately disable a computer, or incorporate a time delay, after which a remote command will direct the infected computer to transmit harmful signals that disrupt other computers. An attack can trigger the automatic transmission of huge volumes of harmful signals that can very rapidly disrupt or paralyze many thousands of other computers throughout the Internet, or severely clog transmission lines with an abundance of bogus messages, causing portions of the Internet to become slow and unresponsive.

Preparation for a cyber crime or cyber espionage computer attack by a hacker may sometimes proceed slowly, or in several phases, before a final attack is initiated that will cause maximum damage. Some compromised computers can become part of an automatic "bot" network, quietly performing espionage by transmitting data or

---

[88] The FBI is investigating what private security experts believe to be the first Internet attack aimed primarily at a single economic sector. The malicious code, discovered in June 2003, contains a list of roughly 1,200 Web addresses for many of the world's largest financial institutions, including J.P. Morgan Chase & Co., American Express Co., Wachovia Corp., Bank of America Corp. and Citibank N.A. "Bugbear" is a polymorphic worm/virus that has keystroke-logging and mass-mailing capabilities, and attempts to terminate various antivirus and firewall programs. Though most major banks do not put sensitive information on the Internet, the worm will attempt to use information captured from a desktop PC to break into restricted computers that do contain financial data. For example, experts found that the Bugbear software is programmed to determine whether a victim used an e-mail address that belonged to any of the 1,300 financial institutions listed in its blueprints. If a match is made, it tries to steal passwords and other information that would make it easier for hackers to break into a bank's networks. The software then transmits stolen passwords to 10 e-mail addresses, which also are included in the blueprints. But experts said that on the Internet anyone can easily open a free e-mail account using a false name, and so knowing those addresses might not lead detectives to the culprit. A.P., June 10, 2003, *Feds Warn Banks About Internet Attack*, CNN.Com, [http://www.cnn.com/2003/TECH/internet/06/10/virus.banks.ap/index.html].

[89] The Naval Postgraduate School is developing a new network security tool called "Therminator", that is designed to detect possible computer attacks by carefully monitoring network traffic. Jason Ma, October 6, 2003, *NPS Touts Therminator As Early-Warning Tool for Computer Attacks*, Inside the Navy, Navy-16-40-12.

intermediate preparatory instructions back and forth between compromised computers, while awaiting a special final activation signal originating from the attacker. The final activation phase may direct all compromised computers to inundate a targeted computer with bogus messages, or insert phony data into critical computer systems, causing them to malfunction at a crucial point, or affect other computers downstream. Some recent computer attacks have focused on only a single new computer vulnerability, and have been seen to spread worldwide through the Internet with astonishing speed.[90]

---

[90] The "Slammer" worm attacked Microsoft's database software and spread through the Internet over one weekend in January 2003. According to a preliminary study coordinated by the Cooperative Association for Internet Data Analysis (CAIDA), on January 25, 2003, the SQL Slammer worm (also known as "Sapphire") infected more than 90 percent of vulnerable computers worldwide within 10 minutes of its release on the Internet, making it the fastest computer worm in history. As the study reports, exploiting a known vulnerability for which a patch has been available since July 2002, Slammer 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 and such unforeseen consequences as canceled airline flights and automated teller machine (ATM) failures. Further, the study emphasizes that the effects would likely have been more severe had Slammer carried a malicious payload, attacked a more widespread vulnerability, or targeted a more popular service. The malicious code disrupted more than 13,000 Bank of America automated teller machines, causing some machines to stop issuing money, and took most of South Korea Internet users offline. As many as five of the 13 Internet root name servers were also slowed or disabled, according to Anti-virus firm F-Secure. Robert F. Dacey, 2003, *INFORMATION SECURITY: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, Matt Loney, 2003, *Computer worm slows global Net traffic,* [http://news.com.com/2102-1001-982131.html,] Robert Lemos,2003, *Worm exposes apathy, Microsoft flaws,* [http://news.com.com/2102-1001-982135.html].

Appendix C - Comparison of Computer Attacks and Terrorist Tactics

Similarities may exist in characteristics of some tactics used to prepare for and execute a cyber crime or cyber espionage computer attack, and tactics used to prepare for and execute some recent physical terrorist operations. For example, (1) network meetings in cyberspace, (2) extensive pre-operative surveillance, (3) exploits of soft and vulnerable targets, and (4) swarming methods may all be characteristics of tactics used by some terrorist groups as well as by computer hackers. Knowing these similarities may be helpful to investigators as they explore different methods to detect planning, and help prevent a possible cyber attack by terrorist groups.

The organizational structures of many terrorist groups are not well understood and are usually intended to conceal the interconnections and relationships.[91] A network organization structure (as opposed to a hierarchical structure) favors smaller units, giving the group the ability to attack and quickly overwhelm defenders, and then just as quickly disperse or disappear. Terrorist groups using a network structure to plan and execute an attack can place government hierarchies at a disadvantage because a terrorist attack often blurs the traditional lines of authority between agencies such as police, the military, and other responders.

Similarly, computer hackers are often composed of small groups or individuals who meet anonymously in network chat rooms to exchange information about computer vulnerabilities, and plan ways to exploit them for cyber crime or cyber espionage. By meeting only in cyberspace, hackers can quickly disappear whenever government authorities try to locate them. Hackers have also designed recent computer exploits that launch anonymously from thousands of infected computers to produce waves of disruption that quickly overwhelm a single targeted organization, or multiple organizations such as a list of banking institutions.

In a similar manner, terrorist groups may also strike in waves from multiple dispersed directions against multiple targets, in swarming campaigns. A non-computer example of swarming may be the May 11, 2003 attack in Riyadh, where terrorists (possibly Al Qaeda), staged simultaneous assaults at three compounds in different locations, with each assault involving a rapid strike with multiple vehicles, some carrying explosives and others carrying gunmen.

Terrorist groups are described by DHS as opportunistic, choosing to exploit soft vulnerabilities that are left exposed. Similarly, an increasingly popular trend for computer hackers engaged in computer crime or computer espionage is to use a malicious program called a worm, that pro-actively spreads copies of itself through the Internet, rapidly finding as many computers as possible with the same non-patched vulnerability, and then automatically installing itself to quietly await further instructions from the attacker.

---

[91] *Report to Congress Regarding the Terrorism Information Awareness Program*, Executive Summary, May 20 2003, p.3.

At an appropriate time, the attacker may choose to send a command through the Internet to activate these thousands of infected computers, instructing them to either stop working properly, or reveal unauthorized information (such as passwords or credit card numbers), or attack and overwhelm a targeted organization and block access to many services on the Internet. A worm can quietly corrupt data on infected computers, transmit that corrupted data to other downstream computers, and even interfere with network response for computers that have installed the right security to protect against infection.