Congressional Research Service

Report RL33123

Terrorist Capabilities for Cyberattack: Overview and Policy Issues

John Rollins and Clay Wilson, Foreign Affairs, Defense, and Trade Division

January 22, 2007

Abstract. This report examines possible terrorists' objectives and computer vulnerabilities that might lead to an attempted cyberattack against the critical infrastructure of the U.S. homeland, and also discusses the emerging computer and other technical skills of terrorists and extremists. Policy issues include exploring ways to improve technology for cybersecurity, or whether U.S. counterterrorism efforts should be linked more closely to international efforts to prevent cybercrime.

Order Code RL33123

CRS Report for Congress

Terrorist Capabilities for Cyberattack: Overview and Policy Issues

Updated January 22, 2007

John Rollins
Specialist in Terrorism and International Crime
Foreign Affairs, Defense, and Trade Division

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

Congressional Research Service

Prepared for Members and Committees of Congress

Terrorist Capabilities for Cyberattack: Overview and Policy Issues

Summary

Terrorist's use of the internet and other telecommunications devices is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. Tighter physical and border security may also encourage terrorists and extremists to try to use other types of weapons to attack the United States. Persistent Internet and computer security vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations and consider attempting a cyberattack against the U.S. critical infrastructure.

Cybercrime has increased dramatically in past years, and several recent terrorist events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money, and for the smuggling of arms and illegal drugs. These links with hackers and cybercriminals may be examples of the terrorists' desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers. The July 2005 subway and bus bombings in England also indicate that extremists and their sympathizers may already be embedded in societies with a large information technology workforce.

The United States and international community have taken steps to coordinate laws to prevent cybercrime, but if trends continue computer attacks will become more numerous, faster, and more sophisticated. In addition, a recent report by the Government Accountability Office states that, in the future, U.S. government agencies may not be able to respond effectively to such attacks.

This report examines possible terrorists' objectives and computer vulnerabilities that might lead to an attempted cyberattack against the critical infrastructure of the U.S. homeland, and also discusses the emerging computer and other technical skills of terrorists and extremists. Policy issues include exploring ways to improve technology for cybersecurity, or whether U.S. counterterrorism efforts should be linked more closely to international efforts to prevent cybercrime.

This report will be updated as events warrant.

Contents

Terrorist Capabilities for Cyberattack: Overview and Policy Issues

Introduction

Often it is very difficult to determine if a cyber attack or intrusion is the work of a terrorist organization with the objective of doing harm, or a cyber criminal who wishes to steal information for purposes of monetary gain. Just as terrorists and violent extremists often rely on exploiting vulnerabilities of targets seen as soft and easy to access to support possible future cyber attacks, cyber criminals exploit these same vulnerabilities to gain access to information that may lead to monetary gain. Implementation of a stronger policy for domestic physical security has reduced the risk to some targets that may have previously been vulnerable to physical attacks. Also, it is suggested by numerous experts that terrorists may be enhancing their computer skills or forming alliances with cybercriminals that possess a high-level of telecommunications expertise. In addition, continuing publicity about Internet computer security vulnerabilities may encourage terrorists' interest in attempting a possible computer network attack, or cyberattack, against U.S. critical infrastructure.

To date, the Federal Bureau of Investigation (FBI) reports that cyberattacks attributed to terrorists have largely been limited to unsophisticated efforts such as email bombing of ideological foes, or defacing of websites. However, it says their increasing technical competency is resulting in an emerging capability for network-based attacks. The FBI has predicted that terrorists will either develop or hire hackers for the purpose of complimenting large conventional attacks with cyberattacks.[1] Recently, during the Annual Threat Assessment, FBI Director Mueller observed that "terrorists increasingly use the internet to communicate, conduct operational planning, proselytize, recruit, train and to obtain logistical and financial support. That is a growing and increasing concern for us."[2]

IBM has reported that, during the first half of 2005, criminal-driven computer security attacks increased by 50 percent, with government agencies and industries in the United States targeted most frequently.[3] Cybercrime is now a major criminal

---

[1] Keith Lourdeau, FBI Deputy Assistant Director, testimony before the U.S. Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, February 24, 2004.

[2] Robert Mueller, FBI Director, testimony before the Senate Select Committee on Intelligence, January 11, 2007.

[3] IBM Press Release, Government, financial services and manufacturing sectors top targets of security attacks in first half of 2005, August 2, 2005,

activity, and it may become increasingly difficult to separate some forms of cybercrime from suspected terrorist activities. For example, in a recent report from the House Homeland Security Committee, FBI officials indicated that extremists have used identity theft and credit card fraud to support recent terrorist activities by Al Qaeda cells.[4] Also, according to press reports Indonesian police officials believe the 2002 terrorist bombings in Bali were partially financed through online credit card fraud.[5]

This report reviews publications and government reports to explore the following: (1) examples of vulnerabilities that may raise the level of interest that terrorists might have in attempting a coordinated cyberattack; (2) effects of the War on Terror that are driving terrorists to use the Internet more; (3) inconsistent reporting about terrorists' cyber activities; and (4) ways that terrorists may be improving their cyber skills.

Background

Distinctions between crime, terrorism, and war tend to blur when attempting to describe a computer network attack (CNA) in ways that parallel the physical world. For example, if a nation state were to secretly sponsor non-state actors who initiate a CNA to support terrorist activities or to create economic disruption, the distinction between cybercrime and cyberwar becomes less clear. Because it is difficult to tell from where a cyberattack originates, an attacker may direct suspicion toward an innocent third party. Likewise, the interactions between terrorists and criminals who use computer technology may sometimes blur the distinction between cybercrime and cyberterrorism. It also may be the case that individuals providing computer expertise to a criminal or terrorist may not be aware of the intentions of the individual that requested the support. So far, it remains difficult to determine the sources responsible for most of the annoying, yet increasingly sophisticated attacks that plague the Internet. Given the difficulty in determining the originator of the cyber intrusions or attacks, some argue that unlike responding to traditional criminal acts, the focus should be on the act rather than the perpetrator and the threshold for launching defensive and offensive actions should be lowered.

---

[3] (...continued)
[http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html].

[4] According to FBI officials, Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases. Also, the FBI has recorded more than 9.3 million Americans as victims of identity theft in a 12-month period; June, 2005. Report by the Democratic Staff of the House Homeland Security Committee, *Identity Theft and Terrorism*, July 1, 2005, p. 10.

[5] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War Into Cyberspace," *Washington Post*, December 14, 2004, p. A19.

The Internet is now used as a prime recruiting tool for insurgents in Iraq.[6] Insurgents have created many Arabic-language websites that are said to contain coded plans for new attacks. Some reportedly give advice on how to build and operate weapons, and how to pass through border checkpoints.[7] Other news articles report that a younger generation of terrorists and extremists, such as those behind the July 2005 bombings in London, are learning new technical skills to help them avoid detection by law enforcement computer technology.[8]

When is Cyberattack Considered Cyberterrorism?

Some observers feel that the term "Cyberterrorism" is inappropriate, because a widespread cyberattack may simply produce annoyances, not terror, as would a bomb, or other chemical, biological, radiological, or nuclear explosive (CBRN) weapon. However, others believe that the effects of a widespread computer network attack would be unpredictable and might cause enough economic disruption, fear, and civilian deaths, to qualify as terrorism. At least two views exist for defining the term Cyberterrorism:

- **Effects-based**: Cyberterrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.
- **Intent-based**: Cyberterrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.[9]

Objectives for a Cyberattack

The Internet, whether accessed by a desktop computer or the many available handheld devices, is the medium through which a cyberattack would be delivered. However, for a targeted attack[10] to be successful, the attackers usually require that the network itself remain more or less intact, unless the attackers assess that the perceived gains from shutting down the network would offset the accompanying loss of communication. A targeted cyberattack could be effective if directed against a

---

[6] Jonathan Curiel, "TERROR.COM: Iraq's tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet," *San Francisco Chronicle*, July 10, 2005, [http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/07/10/CURIEL.TMP].

[7] Jonathan Curiel, "Iraq's tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet," *San Francisco Chronicle*, July 10, 2005, p. A.01.

[8] Michael Evans and Daniel McGrory, "Terrorists Trained in Western Methods Will Leave Few Clues," *London Times*, July 12, 2005.

[9] For a more in-depth discussion of the definition of cyberterrorism, see CRS Report RL32114, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson.

[10] A targeted attack is one where the attacker is intentionally attempting to gain access to or disrupt a specific target. This is in contrast to a random attack where the attacker seeks access to or disrupt any target that appears vulnerable.

portion of the U.S. critical infrastructure, and if timed to amplify the effects of a simultaneous conventional physical or chemical, biological, nuclear, or radiological (CBRN) terrorist attack. The objectives of a cyberattack include the following four areas:[11]

1. Loss of integrity, such that information could be modified improperly;
2. Loss of availability, where mission critical information systems are rendered unavailable to authorized users;
3. Loss of confidentiality, where critical information is disclosed to unauthorized users; and,
4. Physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

According to Richard Clarke, former Administration Counter Terrorism Advisor and National Security Advisor, if terrorists were to launch a widespread cyberattack against the United States, the economy would be the intended target for disruption, while death and destruction might be considered collateral damage.[12] Many security experts also agree that a cyberattack would be most effective if it were used to amplify a conventional bombing or CBRN attack. Such a scenario might include attempting to disrupt 911 call centers simultaneous with the detonating of an explosives devices. This type of example is usually contrasted to a widespread, coordinated cyberattack, unaccompanied by a physical attack, that would technically be very difficult to orchestrate and unlikely be effective in furthering terrorists' goals. Because such an attack cannot directly cause death and destruction, this may explain why there is no evidence that terrorist groups have undertaken a significant cyber attack.[13] However, other observers say that, because of interdependencies among infrastructure sectors, a large-scale cyberattack that affected one sector could also have disruptive, unpredictable, and perhaps devastating effects on other sectors, and possibly long-lasting effects to the economy. These observers assert Al Qaeda and associated terrorist groups are becoming more technically sophisticated, and years of

---

[11] U.S. Army Training and Doctrine Command, Cyber Operations and Cyber Terrorism, Handbook No. 1.02, August 15, 2005, p.II-1 and II-3

[12] Kevin Rademacher reporting remarks of Richard Clarke at CardTech/SecurTech security conference April 2005, "Clarke: ID Theft Prevention Tied to Anti-terrorism Efforts," *Las Vegas Sun*, April 13, 2005, at [http://www.lasvegassun.com/sumbin/stories/text/2005/apr/13/518595803.html].

[13] Joris Evers, "Does Cyberterrorism Pose a True Threat?," *PCWorld*, March 14, 2003, at [http://www.peworld.com/news/article/0,aid,109819,00.asp]. Joris Evers, reporting remarks by Bruce Schneier at CeBIT technology trade show in March 2003, "Cyberterror Threat Overblown," *Computerworld*, March 14, 2003, at [http://www.computeworld,com/printthis/2003/0,4814,79368,00.html]. Gabriel Weimann, *Special Report - Cyberterrorism: How Real is the Threat?*, United States Institute of Peace, Washington, D.C., May 2004. Dan Ilett reporting remarks of Richard Clarke at the Oxford University Internet Institute in February 2005, Clarke joins latest cyberterror debate, ZDNet UK, February 11, 2005, at [http://www.zdnet.co.uk/print/?TYPE=story&AT=39187582-39020375t-10000025c].

publicity about computer security weaknesses has made them aware that the U.S. economy could be vulnerable to a coordinated cyberattack.[14]

Publicity would be also one of the primary objectives for a terrorist attack. Extensive coverage has been given to the vulnerability of the U.S. information infrastructure and to the potential harm that could be caused by a cyberattack. This might lead terrorists to feel that even a marginally successful cyberattack directed at the United States may garner considerable publicity.[15] Some suggest that were such a cyber attack by a terrorist organization to occur and become known to the general public, regardless of the level of success of the attack, concern by many citizens may lead to widespread withdrawal of funds and selling of equities.

Persistent Computer Security Vulnerabilities

At the July 2005 Black Hat computer security conference (a private sector sponsored annual meeting of organizations focused on cyber-security technology and related issues) Las Vegas, a security expert demonstrated an exploit of what many consider to be a significant Internet security flaw, by showing how the most commonly used Internet routers; the computer's device that forwards data to a desired destination, could quickly be hacked.[16] This router vulnerability could allow an attacker to disrupt selected portions of the Internet, or even target specific groups of banks or power stations.[17] Security expert Bruce Schneier, a recent critic of the idea of cyberterrorism, reportedly agreed that the router flaw was a "major" Internet security vulnerability, and could allow criminals to steal identity information, or otherwise attack networks. The company released in April 2005 a software patch to fix the problem, but over the following four months, had apparently not notified its customers and government agencies, including DHS, about the seriousness of the vulnerability.[18]

---

[14] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism*, McGraw-Hill, 2003, p. 110. Keith Lourdeau, Deputy Assistant Director of the FBI Cyber Division, testimony before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security, February 24, 2004. Ryan Naraine reporting remarks of Roger Cressey at Infosec World 2005, *Cyber-Terrorism Analyst Warns Against Complacency*, eWEEK.com, April 4, 2005, at [http://www.eweek.com/article2/0,1759,1782288,00.asp].

[15] The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications, Office of the Manager, National Communications System, December 2000, p.31, at [http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf].

[16] Amy Storer, Update: *IPv6 risks may outweigh benefits*, SearchSecurity.com, July 29, 2005, at [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1112459,00.html?track=NL-358&ad=525032USCA].

[17] Victor Garza, *Security researcher cause furor by releasing flaw in Cisco Systems IOS*, SearchSecurity.com, July 28, 2005, at [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1111389,00.html].

[18] Justin Rood, *Cisco Failed to Alert DHS, Other Agencies About Software Security Flaw*, CQ Homeland Security, August 2, 2005, at [http://homeland.cq.com/hs/display.do?docid=1810432&sourcetype=31&binderName=news-all].

The United States may provide ample economic targets vulnerable to cyberattack, thus tempting terrorist groups to increase their cyber skills.[19] A February 2005 report by the President's Information Technology Committee (PITAC) stated that the information technology infrastructure of the United States, which is vital for communication, commerce, and control of the physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The report also found that the private sector has an important role in protecting national security by deploying sound security products, and by adopting good security practices.[20] However, a recent survey of 136,000 PCs used in 251 commercial businesses in North America found that a major security software patch, known as SP2, was installed on only nine percent of the systems, despite the fact that Microsoft advertized the importance of installing the security patch one year ago. The remaining 91 percent of commercial businesses surveyed will continue to be exposed to major security threats until they deploy the software patch throughout their organizations.[21] This may bring into question the extent to which the private sector will self-protect without greater incentive.

Several recent studies by global computer security firms found that the highest rates for computer attack activity were directed against critical infrastructures, such as government, financial services, manufacturing, and power. These reports also show that the United States is the most highly targeted nation for computer attacks; during the first half of 2005, United States computer systems were attacked at a rate 10 times higher than the next most highly targeted nation, China (see section titled "Trends in Cybercrime," below).[22] U.S. federal agencies have come under criticism in past years for the effectiveness of their computer security programs.[23] Further, a May 2005 report by the Government Accountability Office (GAO) stated that

---

[19] Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism*, McGraw-Hill, 2003, p. 110. (Hereafter cited as Verton, *Black Ice*.)

[20] The President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization*, Report to the President, February 2005, p. 25, [http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf].

[21] John Foley, "Businesses Slow to Deploy Windows XP SP2," *Information Week*, April 26, 2005, p. 26.

[22] IBM News, *Report Finds Online Attacks Shift Toward Profit*, August 2, 2005, at [http://www.ibm.com/news/us/en/2005/08/2005_08_02.html]. Symantec Press Release, S*ymantec Internet Security Threat Report Highlights Rise In Threats To Confidential Information*, March 21, 2005, at [http://www.symantec.com/press/2005/n050321.html].

[23] 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*, at [http://www.washingtonpost.com/ac2/wp-dyn/A12321-2002Nov19?language=printer.]

because of the growing sophistication of malicious code on the Internet, the federal government may increasingly be limited in its ability to respond to cyber threats.[24]

U.S. Government Cybersecurity Efforts

Many U.S. federal government departments and agencies have responsibilities and have established programs to address various aspects of cyber-security. Some would argue that this level of federal effort demonstrates the government's view as recognizing cyber-security as a national priority. Others see the many organizations and programs as unnecessarily duplicative with the Nation lacking a coherent strategy for understanding the true cyber security threat or the roles and responsibilities of each federal government organization.

Department of Homeland Security (DHS). Some homeland security experts are concerned that the establishment of DHS has delayed federal government cyber security efforts significantly. It is suggested that during a time when the terrorists appear to be growing more reliant on the internet and gaining valuable expertise and experience, DHS, the lead federal agency responsible for cyber-security, has not progressed to meet the challenges that might lie ahead. Others cite the difficulty of ascertaining the intentions, origination, and groups behind cyber-intrusions and attacks as a reason for DHS and the federal government's lack of progress. In February, 2006, DHS participated in and sponsored exercise Cyber Storm which tested the ability of the U.S. government, international partners, and the private sector to recognize, disrupt, and respond to a large-scale cyber attack. Analysis of the exercise produced eight major findings to better position the United States to "enhance the nation's cyber preparedness and response capabilities."[25] While many were pleased that DHS conducted this exercise and recognized areas for improvement, other homeland security observers found the findings to be an acknowledgment of the work that has not been accomplished since the establishment of the Department.

Department of Defense. In August 2005, DOD Directive 3020.40, the "Defense Critical Infrastructure Program," assigned functional responsibility within DOD for coordinating with public and private sector services for protection of defense critical infrastructures from terrorist attacks, including cyberattack.[26] DOD also announced the formation of the Joint Functional Component Command for Network Warfare (JFCCNW) which has responsibility for defending all DOD

---

[24] GAO, *Information Security; Emerging Cybersecurity Issues Threaten Federal Information Systems*, report 05-231, May 2005.

[25] DHS, DHS Releases Cyber Storm Public Exercise Report, September 13, 2006 [http://www.dhs.gov/xnews/releases/pr_1158341221370.shtm]. The eight cyber-security enhancement findings addressed: Interagency Coordination, Contingency Planning, Risk Assessment and Roles and Responsibilities, Correlation of Multiple Incidents between Public and Private Sectors, Exercise Program, Coordination between Entities of Cyber Incidents, Common Framework for Response to Information Access, Strategic Communications and Public Relations, and Improvement of Process, Tools and Technology.

[26] The Defense Critical Infrastructure is defined as those DOD and non-DOD networked assets essential to project, support, and sustain military forces and operations worldwide.

computer systems. The expertise and tools used in this mission are for both offensive and defensive operations.[27]

FBI. The FBI Computer Intrusion program provides administrative and operational support and guidance to field offices investigating computer intrusions. A Special Technologies and Applications program supports FBI counterterrorism computer intrusion investigations, and the FBI Cyber International Investigative program conducts international investigations through coordination with FBI Headquarters Office of International Operations and foreign law enforcement agencies.[28]

NSA. The National Security Agency (NSA) has created the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program, which is intended to reduce vulnerability of national information infrastructure by promoting higher education in information assurance (IA), and by producing more professionals with IA expertise. The NSA and the Department of Homeland Security (DHS) in support of the President's National Strategy to Secure Cyberspace, established in February 2003, now jointly sponsor the program. Under this program, four-year colleges and graduate-level universities are eligible to apply to be designated as a National Center of Academic Excellence in Information Assurance Education (CAEIAE). Students attending CAEIAE schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program (SFS).[29]

CIA. The CIA Information Operations Center, which evaluates threats to U.S. computer systems from foreign governments, criminal organizations and hackers, conducted a cybersecurity exercise in 2005 called "Silent Horizon" to see how government and industry could react to Internet based attacks. One problem the CIA wanted to examine was who would actually deal with a major cyberwar attack. In theory, the government is in charge, but in practice, the defenses are controlled by a number of civilian telecommunications firms. The simulated cyber attacks were set five years into the future. The stated premise of the exercise was that cyberspace would see the same level of devastation as the 9/11 hijackings.[30]

An earlier cyberterrorism exercise called "Livewire" concluded there were serious questions over government's role during a cyberattack depending on who was identified as the culprit — terrorists, a foreign government, or bored teenagers. It

---

[27] John Lasker, "U.S. Military's Elite Hacker Crew," *Wired News*, April 18, 2005, [http://www.wired.com/news/print/0,1294,67223,00.html].

[28] Keith Lourdeau, testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, February 24, 2004, [http://www.fbi.gov/congress/congress04/lourdeau022404.htm].

[29] National Security Agency, [http://www.nsa.gov/ia/academia/caeiae.cfm].

[30] Ted Bridis, "'Silent Horizon' war games wrap up for the CIA," *USA Today*, May 26, 2005, [http://www.usatoday.com/tech/news/techpolicy/2005-05-26-cia-wargames_x.htm].

also questioned whether the U.S. government would be able to detect the early stages of such an attack without significant help from private technology companies.

Inter-Agency Forums. To improve cybersecurity for federal agencies and the critical infrastructure, the Office of Management and Budget (OMB) has created a task force to investigate how agencies can better coordinate cybersecurity functions such as training, incident response, disaster recovery, and contingency planning. The U.S. Department of Homeland Security has also created a new National Cyber Security Division that will focus on reducing vulnerabilities in the government's computing networks, and in the private sector to help protect the critical infrastructure.[31]

Many security vendors agree that to combat cybercrime more effectively, it must be treated as a global problem. Some of these security vendors have created their own independent advance-warning systems for their customers through linking proprietary security equipment into global networks that share information collected by their distributed customer base. One example is an early-warning cyber-security intrusion program that's composed of a global network of 19,000 firewall and intrusion-detection devices maintained by thousands of volunteer data partners. This early intrusion system correlates global data to detect the start of a possible swarming Internet attack originating simultaneously in different parts of the world, and notifies administrators to help them defend their systems when targeted.[32] A similar public/private partnership security warning program was created through the Cyber Incident Detection Data Analysis Center (CIDDAC).[33] In 2005, CIDDAC will install special sensors on the networks of participating partner companies to automatically detect cyberattacks and notify administrators and law enforcement.

Changing Concerns about Cyberattack, 2001-2006

Following the September 11 attacks, public concerns were high about the threat of a possible follow-on cyberattack from terrorist groups.[34] Subsequently, there has been disagreement among security experts about (1) whether such an attack could

---

[31] Jason Miller, "New Cybersecurity Team Meets this Week," *Government Computer News*, March 21, 2005. Grant Gross, "Homeland Security to Oversee Cybersecurity," *PC World*, June 9, 2003, at [http://www.pcworld.com/news/article/0,aid,111066,00.asp].

[32] Paul Roberts, "Symantec Offers Early Warning of Net Threats," *PC World*, February 12, 2003, at [http://www.pcworld.com/news/article/0,aid,109322,00.asp].

[33] CIDDAC is a not-for-profit organization that combines private and government perspectives to facilitate automated real-time sharing of cyberattack data. CIDDAC is specifically designed to protect privacy rights while collecting cyber threat information from sensors attached to corporate computer networks.

[34] In July 2002, Gartner Research and the U.S. Naval War College hosted a three-day, seminar-style war game called "Digital Pearl Harbor" (DPH), with the result that 79% of the gamers said that a strategic cyberattack against the United States was likely within the next two years. Gartner Research, 'Digital Pearl Harbor': Defending Your Critical Infrastructure, October 4, 2002, at [http://www.gartner.com/pages/story.php.id.2727.s.8.jsp].

possibly be launched by terrorists against U.S. civilian critical infrastructure, or (2) whether such an attack could seriously disrupt the U.S. economy.[35]

Simulated cyberattacks, conducted by the U.S. Naval War College in 2002, indicated that attempts to cripple the U.S. telecommunications infrastructure would be unsuccessful because system redundancy would prevent damage from becoming too widespread. Many observers suggest that evidence from natural disasters shows that many the critical infrastructure systems, including banking, power, water, and air traffic control, would likely recover rapidly from a possible cyberattack.[36]

To date, there has been no published report of a coordinated cyberattack launched against the critical infrastructure by a terrorist or terrorist group. Dennis McGrath of the Institute of Security Technology Studies at Dartmouth College reportedly observed that, "We hear less and less about a digital Pearl Harbor. Cyberterrorism is not at the top of the list of discussions."[37]

In May 2005, the CIA reportedly conducted a classified war game, dubbed "Silent Horizon," to practice defending against a simulated widespread cyberattack directed against the United States. The national security simulation was considered significant because many U.S. counterterrorism experts feel that far-reaching effects from a cyberattack are highly unlikely.[38] However, other observers believe that tests of countermeasures, even for unlikely events, may sometimes be prudent.

Many cyber security observers are concerned that U.S. government efforts to date have not effectively prepared the nation for a catastrophic cyberattack. A Business Roundtable report issued in June 2006 found three "cyber-gaps" that are keeping the United States from being prepared to recognize and respond to a cyberattack: (1) the lack of established indicators that would indicate an attack is underway; (2) a failure to identify who is responsible for restoring affected infrastructure; and (3) a lack of dedicated resources to assist in returning cyber

---

[35] Robert Gates, former CIA director, warned that the threat of cyberterrorism should be taken particularly seriously. Keith Lourdeu, deputy assistant director of the FBI Cyber Division, stated that "our networked systems make inviting targets for terrorists due to the potential for large-scale impact on the nation." Douglas Schweitzer, "Be Prepared for Cyberterrorism," *Computerworld*, April 6, 2005. However, others believe that infrastructure systems are robust and could recover quickly. Richard Forno, "Shredding the Paper Tiger of Cyberterrorism," *Security Focus*, September 25, 2002, at [http://www.securityfocus.com/printable/columnists/111]. See also, CRS Report RL32114, *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, by Clay Wilson.

[36] Scott Nance, "Debunking Fears: Exercise Finds 'Digital Pearl Harbour' Risk Small," *Defense Week*, April 7, 2003, at [http://www.kingpublishing.com/publications/dw/]. William Jackson, "War College Calls Digital Pearl Harbor Doable," *Government Computer News*, August 23, 2002, at [http://www.gcn.com/vol1_no1/daily-updates/19792-1.html].

[37] "CIA Overseeing 3-Day Wargame on Internet," *Associated Press*, May 25, 2005.

[38] Ted Bridis, "'Silent Horizon' War Games Wrap up for the CIA," *USA Today*, May 26, 2005, at [http://www.usatoday.com/tech/news/techpolicy/2005-05-26-cia-wargames_x.htm].

operations to a pre-attack condition.[39] Due to increased security measures applied to physical facilities and U.S. government efforts to track and engage groups in their home countries, many believe the internet will increasingly play a bigger role in terrorist support and operational efforts. Many observers that monitor the Internet suggest that due to the effects of intensified counterterrorism efforts worldwide, Islamic extremists are gravitating toward the Internet, and are succeeding in organizing online where they have been failing in the physical world. Terrorist groups increasingly use online services for covert messaging, through steganography, anonymous e-mail accounts, and encryption.[40]

Inconsistent Reporting of Terrorists' Cyber Activities

Some security observers argue that a lack of consistent reporting on the true nature of the cyber-security threat is a direct by-product of the federal government's lack of strategy and inability to clarify assignments for the numerous departments and agencies that have some responsibility for the issue. Others note that the numerous recent governmental organizations are the reason for the delay in progress, and also predict that as DHS and the Office of the Director of National Intelligence mature, the issue of cyber-security assessments and reporting may receive a higher priority.

A review of two annual U.S. government reports on terrorism activity shows inconsistent attention to the issue of possible cyberterrorism.[41] Two federal agencies report on terrorism activity annually: (1) the Department of State's (DOS) *Patterns of Global Terrorism*[42] and, (2) the Federal Bureau of Investigation's *Annual Terrorism in the United States*.[43]

In the DOS reports for the years 1996 to 1999, brief mention is made of cyberterrorism issues. In the year 2000, the report acknowledges that "widespread availability of hacking software and its anonymity and increasingly automated design make it likely that terrorists will more frequently incorporate these tools into their online activity." In 2001, however, no mention of cyberterrorism issues appeared in

---

[39] Business Roundtable, *Essential Steps to Strengthen America's Cyber Terrorism Preparedness*, June 2006, at [http://www.businessroundtable.org/pdf/20060622002CyberReconFinal6106.pdf].

[40] Terrorist suspects are reportedly using encryption techniques to prevent police from accessing vital intelligence on seized computers, according to U.K. police. Stewart Tendler, "Encrypted Files Frustrate Police," *Times Online*, July 20, 2005, at [http://technology.timesonline.co.uk/article/0,,20409-1701405,00.html]. See CryptoHaven, at [http://www.cryptoheaven.com/], and SecretMaker, at [http://www.secretmaker.com/emailsecurer/steganography/default.html].

[41] John Rollins, Specialist in Terrorism and International Crime, Congressional Research Service, August 2005.

[42] "Country Reports on Terrorism" is submitted in compliance with Title 22 of the United States Code, Section 2656(f) which requires the Department of State to provide Congress with a full and complete annual report on terrorism for those countries and groups meeting the criteria of Section (a)(1) and (2) of the act, at [http://www.state.gov/s/ct/rls/c14812.htm].

[43] [http://www.fbi.gov/publications.htm].

the DOS report, and for the years 2002 to 2004, only mentions of various security forums and international cybersecurity working groups were noted.

The FBI's *Annual Terrorism Report* similarly was inconsistent in mentioning cyberterrorism issues. In the 1996 and 1997 reports, there was no mention of cyberterrorism or related activity. In 1998 the report acknowledged that "cyber tools may find their way in the hands of terrorist" and speculated that "the spread of cyberattack tools, like the proliferation of conventional weapon technology may eventually wind up in the hands of terrorists." The following year, 1999, the Report stated that "the threat of cyberterrorism will grow in the new Millennium, as the leadership positions in extremist organizations are increasingly filled with younger, Internet-savvy individuals." These two reports arguably suggested that the issue of cyberterrorism was being followed closely. The Reports from 2000 to 2003 mentioned cyberterrorism, but only in the programmatic aspect regarding organizational changes the FBI was putting in place to address cybersecurity, with no mention of past or projected cyberterrorism incidents or issues. The FBI did not produce a report in 2004, and one is not yet due for 2005.

Since the attacks of 9/11, many observers are concerned that increased efforts to safeguard facilities, infrastructure, personnel safety, and the decrease in the DOS's and FBI's discussion of cybersecurity issues, together may indicate a lack of appreciation for the threat that may be facing the United States from possible cyberterrorism. Others suggest that although the frequency and severity of cyberattacks are on the rise, the federal government may not be sufficiently increasing its efforts to improve cybersecurity.[44]

Technical Skills of Terrorists

Through captured literature, it is known that many Al Qaeda members are well educated, and have familiarity with engineering and other technical areas.[45] During a November 2001 attack by U.S. forces, Al Qaeda fighters fled from Kabul, Afghanistan leaving behind many documents and sensitive information that yielded a profile of some Al Qaeda operatives as well-educated and trained in the use of computer systems. "Technical treatises in Arabic, English, German as well a students' notebooks in Arabic, Turkish, Kurdish, and Russian reflected a consistent interest in and widespread familiarity with electrical and chemical engineering, atomic physics, ballistics, computers, and radios," according to researchers and journalists who reportedly examined the documents.[46]

Just as people all over the world now use the Internet, terrorists also use it as a modern tool for communication. Terrorists and extremist groups have reportedly

---

[44] GAO, *Information Security; Emerging Cybersecurity Issues Threaten Federal Information Systems*, report 05-231, May 2005.

[45] Tom Spring, "Al Qaeda's Tech Traps," *PC World*, September 1, 2004, [http://www.pcworld.com/news/article/0,aid,117658,00.asp].

[46] Anthony Davis, "The Afghan files: Al-Qaeda Documents from Kabul," *Jane's Intelligence Review*, February 1, 2002.

generated thousands of Internet web sites to support psychological operations, fund raising, recruitment, and coordination of activities. Recently, the Department of State's Counterterrorism Director noted "the most worrisome scenario of another attack in the homeland is lone operatives who slip into the country and take directions through cyberspace."[47] A significant concern is that some of these web sites used for the suspected terrorist activity are hosted on Internet Service Providers inside the United States.[48] The level of technical sophistication of the extremist groups that use and operate these web sites has also increased. In 2006 it was reported that an organization linked to al-Qaeda produced a 26-page manual providing instructions on the use of the Google search engine to further the goals of global jihad.[49] Recently British forces in Iraq have found print-outs of Google-Earth pictures that reportedly were to be used for targeting of coalition forces.[50]

A recent study of more than 200,000 multimedia documents on 86 sample websites concluded that extremists exhibited similar levels of web knowledge as U.S. government agencies, and that the terrorist websites employed significantly more sophisticated multimedia technologies than U.S. government websites. The study concluded that these extremist websites support advanced Internet-based communication tools such as online forums and chat rooms more frequently than U.S. government web sites.[51] Because of perceived anonymity, terrorist likely feel safer when working together on the Internet.

In April 2002, the Central Intelligence Agency (CIA) stated in a letter to the U.S. Senate Select Committee on Intelligence that cyberwarfare attacks against the U.S. critical infrastructure will become a viable option for terrorists as they become more familiar with the technology required for the attacks. Also according to the CIA, various groups, including Al Qaeda and Hizballah, are becoming more adept at using the Internet and computer technologies, and these groups could possibly develop the skills necessary for a cyberattack.[52] In February 2005, FBI director Robert Mueller, testified before the Senate Select Committee on Intelligence that terrorists show a growing understanding of the critical role of information technology

---

[47] Michael Isikoff, Terror: We're Going to Get Hit, *Newsweek*, January 22, 2007.

[48] Internet Service Providers (ISPs) are not liable for terrorist propaganda posted on their systems unless they have actual knowledge of it. Once discovered, terrorist web sites can quickly jump to another ISP faster than system administrators, or law enforcement, can track them. Evan Kohlman, Al Qaeda on the Internet, *Washington Post online interview*, August 8, 2005, 3 P.M. E.T.

[49] "Terrorists Launch Google Guide," *The Jawa Report*, November 29, 2006, [http://mypetjawa.mu.nu/archives/185504.php].

[50] Thomas Harding, "Terrorists use Google Maps to hit UK Troops," *Telegraph*, January 13, 2007, [http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml].

[51] Jialun Qin et al., Analyzing terror campaigns on the internet: Technical sophistication, content richness, and Web interactivity, International Journal of Human-Computer Studies, November 1, 2006, vol. 65, p.71-84.

[52] Verton, *Black Ice*, p. 87.

in the U.S. economy and have expanded their recruitment to include people studying math, computer science, and engineering.[53]

Senior leadership of al-Qaeda, who reportedly have access to the most modern technology equipment,[54] and other terrorist groups are reportedly building a massive and dynamic online library of training materials, many of which are supported by subject matter experts who answer questions on message boards or in chat rooms. This online library covers such areas as how to mix poisons for chemical attacks, how to ambush U.S. soldiers, how to coordinate a suicide bomb attack, and how to hack computers.[55] One discussion forum popular with supporters of terrorism is called Qalah, or Fortress, where potential al Qaeda recruits can find links to the latest in computer hacking techniques in a discussion area called "electronic jihad."[56]

Some security experts do not think it is worthwhile to hijack or disrupt the web sites created by terrorists. This is because terrorists will usually find a way to quickly put their sites back up under different, multiple names, which may be even more difficult to monitor. Instead, U.S. intelligence sources can gain valuable information by simply monitoring the web sites they already know about. This may also include monitoring the Internet addresses of those who frequent these web sites. However, more skilled analysts are needed to help translate the communications and information that is posted on the many different terrorist web sites.[57]

The *Washington Times* has reported that Islamic extremists are calling for creation of an Islamist hackers' army to plan cyberattacks against the U.S. government and that postings on the extremist bulletin board, al-Farooq, carry detailed cyberattack instructions, and include spyware programs for download that can be used to learn the passwords of targeted users.[58] Other extremist websites reportedly resemble online training camps that may offer instructions for how to create a safe-house, how to clean a rocket-propelled grenade launcher, or what to do if captured.[59]

---

[53] Testimony before the Senate Select Committee on Intelligence, February 16, 2005.

[54] "Al-Qaida leaders have the best computer technology that money can buy." Evan Kohlmann, terrorism consultant, *Newsday*, Tunnel Plot Talk in Web Chat rooms can net cyber terrorists, July 8, 2006.

[55] Some have described these web training sites as an open university for jihad. Steve Coll and Susan Glasser, "Terrorists Turn to the Web as Base of Operations," *Washington Post*, Aug 7, 2005, A1.

[56] Steve Coll and Susan Glasser, "Terrorists Turn to the Web as Base of Operations," *Washington Post*, Aug 7, 2005, A1.

[57] Susan Glassar, "The Iraq Insurgency's Online Strategy," *Washington Post online interview*, August 9, 2005, 11 A.M. E.T.

[58] Shaun Waterman, "Islamists Seek To Organize Hackers' Jihad in Cyberspace," *Washington Times*, August 26, 2005, p. 9.

[59] Tom Spring, "Al Qaeda's Tech Traps," *PCWorld*, September 1, 2004, at [http://www.pcworld.com/news/article/0,aid,117658,00.asp].

Iman Samudra, convicted and now awaiting execution for taking part in the 2002 bombings of two Bali nightclubs, has written a book titled "Aku Mekawan Terroris!", which reportedly translates to "Me Against the Terrorist". Samudra advocates that Muslim youth actively develop hacking skills "to attack U.S. computer networks." Samudra names several websites and chat rooms as sources for increasing hacking skills. He urges Muslim youth to obtain credit card numbers and use them to fund the struggle against the United States and its allies.[60] The terrorist attacks in Bali, and recent attacks in several other countries, may have been funded through stolen credit cards.[61]

Cyberterrorism Capability of State Sponsors of Terrorism

Methods for conducting information warfare to advance the goals of a nation state might also involve secretly sponsoring terrorists. In March 2005, a Department of Homeland Security (DHS) report indicated that, of the six nations currently listed by the State Department as terrorist sponsors, five of them — North Korea, Sudan, Syria, Libya, and Cuba — are described as a diminishing concern for terrorism. Only Iran remains listed as a nation-state possibly having a future motivation to assist terrorist groups in attacking the United States homeland. However, some experts believe that a decline in state-sponsorship of terrorism may push terrorist organizations to increasingly embrace the drug trade or other forms of cybercrime.[62]

China is often cited as providing government support to computer-hackers. A paper published in 1999 authored by two senior colonels in the Chinese military specifically discusses the need for China to place new emphasis on information warfare methods to attack enemy financial markets, civilian electricity networks, and telecommunications networks by burying "... a computer virus and hacker detachment in the opponent's computer systems in advance..." of launching the information warfare network attacks.[63]

DOD officials have acknowledged that hackers, apparently based in China, have been successfully penetrating U.S. military networks since 2001, and perhaps earlier. Although some of these successful cyberattacks were directed against unclassified networks, one intrusion reportedly did obtain data about a future Army command and

---

[60] FBI Report FEA20041222000744, version 17, *Convicted Indonesian Terrorist Calls for Computer Hacking, Jihad Against US*, December 4, 2004, [https://www.fbis.gov/portal/server.pt/gateway/PTARGS_0_22439_246_203_0_43/http%3B/apps.fbis.gov%3B7011/fbis.gov/search/Search?action=viewDocument&holding=5051585].

[61] Richard Clarke, former counterterrorism advisor for Presidents George W. Bush and Bill Clinton, stated that we are vulnerable to people who would use our identities against us. Kevin Rademacher, "Clarke: ID Theft Prevention Tied to Anti-Terrorism Efforts, *Las Vegas Sun*, April 13, 2005, at [http://www.lasvegassun.com/sunbin/stories/text/2005/apr/13/518595803.html].

[62] Jennifer Hesterman, *Transnational Crime and the Criminal-Terrorist Nexus*, Walker Paper No.1, Air University, Air University Press, May, 2005, p.32.

[63] Qioa Lang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999.

control system.[64] Although the hackers are suspected to be based in China, DOD and security officials remain divided over (1) whether the ongoing cyberattacks are coordinated or sponsored by the Chinese government, (2) whether they are the work of individual and independent hackers, or (3) whether the cyberattacks are being initiated by some third-party organization that is using network servers in China to disguise the true origins of the attacks. It remains very difficult to determine the true identity, purpose, or sponsor (if any) of a cyber attacker.

Trends in Cyberterrorism and Cybercrime

Today, cyberattacks are increasingly designed to silently steal information without leaving behind any damage that would be noticeable to a user. These types of attacks attempt to escape detection in order to remain on host systems for longer periods of time. Research has shown that attackers are now focusing their efforts on infecting home user desktops or taking control of web applications, allowing the attacker to steal confidential information such as passwords or account codes. The attackers are also using new malicious code tools called "bot networks" that attempt to deny Internet service to targeted victims. According to recent studies by the security organization Symantec and the Cyber Security Industry Alliance, in the first six months of 2006 the home user sector accounted for a large percentage of all targeted attacks, and many home users now believe their financial and personal information may be at risk due to cybercrime.[65]

Identity theft involving thousands of victims is enabled by advances in computer technology, and by poor computer security practices.[66] In June 2006, officials from the U.S. Department of Energy acknowledged that names and personal information belonging to more than 1,500 employees of the National Nuclear Security Administration (NNSA) had been stolen in a network intrusion that apparently took place starting in 2004. The NNSA did not discover the security breach until one year after it had occurred.[67]

---

[64] Frank Tiboni, "The New Trojan War," *Federal Computer Week*, August 22, 2005, p. 60. Nathan Thornburgh, *Inside the Chinese Hack Attack*, August 25, 2005, at [http://www.time.com/time/nation/printout/0,8816,1098371,00.html].

[65] Vincent Weafer, Statement before the House Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, September 13, 2006.

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

[67] Dawn Onley and Patience Wait, DOD's efforts to stave off nation-state cyberattacks begin with China, *Government Computer News*, August 21, 2006.

A series of computer attacks launched in 2003 against DOD systems and computer systems belonging to DOD contractors apparently went undetected for many months. This series of cyberattacks was labeled "Titan Rain," and was suspected by DOD investigators to originate in China. The attacks were directed against the U.S. Defense Information Systems Agency (DISA), the U.S. Redstone Arsenal, the Army Space and Strategic Defense Installation, and several computer systems critical to military logistics. Although no classified systems were breached, many files were copied containing information that is sensitive and subject to export-control laws.

In November 2006, an extended computer attack against the U.S. Naval War College in Newport, Rhode Island, prompted officials to disconnect the entire campus from the Internet.[68] DOD officials acknowledge that the Global Information Grid, which is the main network for the U.S. military, experiences more than three million daily scans by unknown potential intruders. DOD officials also suspect that most of these scans originated in the United States and in China (although some of the attacks apparently only traversed through networks in China, casting some doubt on the true origin).[69]

Security experts warn that all U.S. federal agencies should now be aware that in cyberspace some countries consider that no boundaries exist between military and civilian targets. According to an August 2005 computer security report by IBM, more than 237 million overall security attacks were reported globally during the first half of the year.[70] Government agencies were targeted the most, reporting more than 54 million attacks, while manufacturing ranked second with 36 million attacks, financial services ranked third with approximately 34 million, and healthcare received more than 17 million attacks. The most frequent targets for these attacks, all occurring in the first half of 2005, were government agencies and industries in the United States (12 million), followed by New Zealand (1.2 million), and China (1 million). These statistics may represent an underestimation, given that most security analysts agree that the number of incidents reported are only a small fraction of the total number of attacks that actually occur.

Usually, a cyberattack is difficult to detect until after it is well underway, and may involve hundreds or thousands of compromised computers from all parts the globe that are directed by a cybercriminal to attack as a swarm. If the attack is directed against a yet-undisclosed, or newly-discovered security vulnerability, the targeted computer systems may be at a significant disadvantage. Most commercial computer security safeguards operate mainly to prevent the types of attacks that are

---

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

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

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

already known to administrators. A new, unique type of attack against computers may encounter inadequate, untested, or non-existent defenses.

A 2004 survey by an internet security company, covering 450 networks in 35 countries, found that hacking had become a profitable criminal pursuit.[71] Hackers sell unknown computer vulnerabilities (commonly called "zero-day exploits") on the black market to criminals who use them for fraud. Hackers with networks of compromised computers (also known as "bot nets") rent them to other criminals who use them to launch coordinated attacks against targeted individuals or businesses, including banks or other institutions that manage financial information.[72]

It has been reported that stolen credit card numbers and bank account information are now traded online in a highly structured arrangement, involving buyers, seller, intermediaries, and service industries. These services include offering to conveniently change the billing address of a theft victim, through manipulation of stolen PINs or passwords. Estimates by some observers are that, in a highly profitable black market, each stolen MasterCard number can be sold for between $42 and $72.[73]

MasterCard International reported that in 2005 more than 40 million credit card numbers belonging to U.S. consumers were accessed by computer hackers and were at risk of being used for fraud.[74] Some of these account numbers were reportedly being sold on a Russian website, and some consumers have reported fraudulent charges on their statements. Officials at the UFJ bank in Japan reportedly stated that some of that bank's customers may also have become victims of fraud related to theft of MasterCard information.[75]

In Autumn 2004, organized cybercriminals appear to have infiltrated the computer systems of the London offices of Sumitomo, the Japanese bank, in an attempt to steal £220 million. The cybercriminals reportedly planned to transfer the money to other bank accounts around the world. Officials at the London police fraud squad reportedly stated that Sumitomo is the only incident so far in which an attack

---

[71] Counterpane Internet Security, *Attack Trends 2005*, June 2005, at [http://www.schneier.com/essay-085.pdf].

[72] Bruce Schneier, *Attack Trends: 2004 and 2005*, June 6, 2005, at [http://www.schneier.com/blog/archives/2005/06/attack_trends_2.html].

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

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

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

by external cybercriminals has nearly succeeded against a major bank.[76] Figures from the National Hi-Tech Crime Unit in England show that, in 2003, at least 83% of U.K. companies were targeted by hackers in attempts to seize control of their systems.[77]

The Insider Threat

A 2003 study of security incidents, conducted by the U.S. Secret Service and the Carnegie Mellon Software Engineering Institute, found that attacks on computer systems committed by insiders with authorized access, have reportedly cost industry millions of dollars in fraud and lost data.[78] Insider employees with access to sensitive information systems can initiate threats in the form of malicious code inserted into software that is being developed either locally, or under offshore contracting arrangements. For example, in January 2003, 20 employees of subcontractors working in the United States at the Sikorsky Aircraft Corporation were arrested for possession of false identification used to obtain security access to facilities containing restricted and sensitive military technology. All of the defendants pleaded guilty and have been sentenced, except for one individual who was convicted at trial on April 19, 2004.[79]

Links Between Terrorism and Cybercrime

The proportion of cybercrime that can be directly or indirectly attributed to terrorists is difficult to determine. Linkages between criminal and terror groups may allow terror networks to expand and undertake large attacks internationally by leveraging criminal sources, money, and transit routes. For example, observers speculate that Aftab Ansari, a criminal suspect located in Dubai, used ransom money earned from prior kidnappings to assist with funding for the September 11, 2001 terrorist attacks. Also, London police officials believe that terrorists obtained the high-quality explosives used for the 2005 bombings through involvement with an Eastern European black market.[80] The recent subway and bus bombings in the U.K. also indicate that groups of terrorists may be active within other countries that have large computerized infrastructures, along with a large, highly skilled information technology workforce. A report by the Department of Homeland Security (DHS) predicts that other possible sponsors of terrorist attacks against the United States homeland may include groups such as Jamaat ul-Fuqura, a Pakistani-based

---

[76] Conal Walsh, "Terrorism on the Cheap — and with No Paper Trail," *The Guardian Observer* (London), July 17, 2005. (Hereafter cited as Walsh, *Terrorism on the Cheap*.)

[77] *Hi-Tech Crime: The Impact on U.K. Business 2005*, 2004 Survey, at [http://www.nhtcu.org/media/documents/publications/8817_Survey.pdf].

[78] Marisa Randazzo et al., *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, Carnegie Mellon Software Engineering Institute, August 2004.

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

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

organization allegedly linked to Muslims of America; Jamaat al Tabligh, an Islamic missionary organization; and, the American Dar Al Islam Movement.[81]

Officials of the U.S. Drug Enforcement Agency (DEA), reported in 2003 that 14 of the 36 groups found on the U.S. State Department's list of foreign terrorist organizations were involved in drug trafficking. Consequently, DEA officials reportedly argued that the war on drugs and the war on terrorism are and should be linked.[82] A 2002 report by the Library of Congress Federal Research Division, revealed a "growing involvement of Islamic terrorist and extremists groups in drug trafficking", and limited evidence of cooperation between different terrorist groups involving both drug trafficking and trafficking in arms.[83] State Department officials, at a Senate hearing in March 2002, also indicated that some terrorist groups may be using drug trafficking as a way to gain financing while simultaneously weakening their enemies in the West through exploiting their desire for addictive drugs.[84] Western Europe and North America continue to be regions that have major narcotics markets, optimal infrastructure, and open commercial nodes that increasingly serve the transnational trafficking needs of both criminal and terrorist groups.[85]

Drug traffickers are reportedly among the most widespread users of computer messaging and encryption, and often have the financial clout to hire high level computer specialists capable of using steganography (writing hidden messages contained in digital photographs) and other means to make Internet messages hard or impossible to decipher. Access to such high level specialists can allow terrorist organizations to transcend borders and operate internationally without detection.

---

[81] The DHS report, dated January 2005, is entitled "Integrated Planning Guidance, Fiscal Years 2005-2011." Justin Rood, "Animal Rights Groups and Ecology Militants Make DHS Terror List, Right-Wing Vigilantes Omitted," *CQ Homeland Security*, March 25, 2005. Eric Lipton, "Homeland Report Says that Threat From Terror-List Nations Is Declining," *The New York Times*, March 31, 2005, p. A9.

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

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

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

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

Many highly trained technical specialists available for hire are located in the countries of the former Soviet Union and in the Indian subcontinent. Some specialists will not work for criminal or terrorist organizations willingly, but may be misled or unaware of their employers political objectives. Still, others will agree to provide assistance because well-paid legitimate employment is scarce in their region.[86]

An emerging area of concern is the involvement of terrorist groups in counterfeiting of intellectual property, which can be even more lucrative than drug trafficking. In other areas, where criminals and terrorists work together to move money internationally, members of terrorist groups may be given special training in computer software, or in engineering, to facilitate communications through the Internet. In-house financial specialists and experienced advisors may also knowingly, or sometimes unknowingly, help cybercriminals evade the scrutiny of bank regulators and international investigators. These reportedly may include, accountants, bank employees in offshore zones and in major financial centers who may or may not also be terrorists or supportive of the political motives of their clients.[87]

International Efforts to Prevent Cybercrime

Cybercrime is a major international challenge, however attitudes about what composes a criminal act of computer wrongdoing may still vary from country to country. The European Union has set up the Critical Information Infrastructure Research Coordination Office (CI2RCO), which is tasked to examine how its member states are protecting their critical infrastructures from possible cyberattack. The project will identify research groups and programs focused on IT security in critical infrastructures.

The Convention on Cybercrime was adopted in 2001 by the Council of Europe, a consultative assembly of 43 countries, based in Strasbourg. The Convention, effective July 2004, is the first and only international treaty to deal with breaches of law "over the internet or other information networks." The Convention requires participating countries to update and harmonize their criminal laws against hacking, infringements on copyrights, computer facilitated fraud, child pornography, and other illicit cyber activities.[88] To date, eight of the 42 countries that signed the Convention have completed the ratification process.

---

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

[87] Louise I. Shelley and John T. Picarelli, "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism," *Police Practice and Research*, vol. 3, no. 4, 2002 p. 311, at [http://www.american.edu/traccc/Publications/Shelley%20Pubs/To%20Add/MethodsnotMotives.pdf].

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

Although the United States has signed the Convention, it did not sign a complementary protocol that contained provisions to criminalize xenophobia and racism on the Internet, which would likely not be supported by the U.S. Constitution.[89] The complementary protocol could be interpreted as requiring nations to imprison anyone guilty of "insulting publicly, through a computer system" certain groups of people based on characteristics such as race or ethnic origin, a requirement that could make it a crime to e-mail jokes about ethnic groups or question whether the Holocaust occurred. The Department of Justice has said that it would be unconstitutional for the United States to sign that additional protocol because of the First Amendment's guarantee of freedom of expression. The Electronic Privacy Information Center, in a June 2004 letter to the Foreign Relations Committee, objected to U.S. ratification of the Convention, because it would "would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards."[90] However, a coalition of U.S. industry associations, including the Business Software Alliance, the Cyber Security Industry Alliance, the American Bankers Association, the Information Technology Association of America, InfraGard, Verisign, and several others, have urged the U.S. Senate Foreign Relations Committee to recommend ratification of the Convention.[91]

The Bush Administration submitted the Convention on Cybercrime (Treaty Doc. 108-11) to the Senate for hearings and resolution in November 2003. On July 26, 2005, the U.S. Senate Foreign Relations Committee approved the signed Convention. The United States will comply with the Convention based on existing U.S. federal law; and no new implementing legislation will be required. Legal analysts say that U.S. negotiators succeeded in scrapping most objectionable provisions, thereby ensuring that the Convention tracks closely with existing U.S. laws.[92]

Analysis and Policy Issues

Computer security experts disagree about whether a widespread coordinated cyberattack by terrorists is a near-term or long-term possibility. However, terrorists have repeatedly demonstrated a willingness to plan and launch conventional attacks against targets that have easy accessibility and numerous vulnerabilities. Internet and

---

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

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

[91] Patience Wait, "Industry Groups Urge Senate Ratification of Cybercrime Treaty," *Government Computer News*, June 6, 2005, at [http://appserv.gcn.com/vol1_no1/web/36257-1.html]. Declan McCullagh, *Tech Firms call for approval of cybercrime treaty*, Cnet News.com, June 29, 2005, at [http://news.com.com/2102-7348_3-5768462.html?tag=st.util.print].

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

computer system vulnerabilities are persistent and widely publicized. As technology continues to advance, the capability, reliance, and interdependent nature of computer systems likely will be more vulnerable to cyberattack tools that are becoming faster and more sophisticated. Terrorists may also be developing links with cybercriminals that will give them access to high-level computer skills. The time may be approaching when a cyberattack may offer advantages that cause terrorists to act, even if the probability of success, or level of effectiveness, is unknown. Similar to terrorists reconnaissance of physical targets to assess the level of security prior to an attack, it is suggested that the U.S. may experience a number of small cyber intrusion events prior to an attempt at a larger more devastating attack.

Given the ability of a catastrophic cyber-attack to disrupt a significant portion of the nation's infrastructure, some national security observers suggest that the Director of National Intelligence (DNI) should have the responsibility for monitoring the capabilities and identities of the countries and groups that may wish to cause the Nation harm through cyberattack. The DNI, as the Nation's Chief Intelligence Officer, has the ability to coordinate all known cyber-threat related information and then task the intelligence community to collect information to better understand the groups that may wish to cause the U.S. harm, and to forecast their intentions and capabilities.

One issue is whether DHS has done enough to strengthen computer security for civilian federal agencies and for the private sector. In July 2005, DHS Secretary Michael Chertoff announced creation of the new position of Assistant Secretary for Cyber and Telecommunications Security. In doing so he acknowledged both the efficiencies and vulnerabilities of modern technology upon which so much of society now depends.[93] Many cybersecurity observers hope that by elevating the DHS Cyber Security Officer from a Division Director to an Assistant Secretary level position, the new senior official will become a more effective proponent of federal government efforts to address and manage information technology vulnerabilities, incident response programs, and remediation efforts.

DHS is also supporting efforts to encourage U.S. computer systems to change to the new, reportedly more secure, IPV6 Internet Protocol.[94] Despite these efforts, according to GAO officials, DHS does not have an Internet recovery plan, or a national cybersecurity threat assessment. DHS officials have stated that a draft cybersecurity threat evaluation plan will be available in late 2005, but a finalized cybersecurity plan that pinpoints the nations's weakest security links will likely not be available until 2006.[95] Leaders of the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Financial Management, Government

---

[93] Secretary Michael Chertoff, U.S. Department of Homeland Security, Second Security Stage Review Remarks, July 13, 2005, at [http://www.dhs.gov/dhspublic /interapp/speech_0255.xml].

[94] IPV6 is the designation for a newer, more secure communications protocol for the Internet. For more information, see CRS Report RL32411, *Network Centric Warfare: Background and Oversight Issues for Congress*, by Clay Wilson.

[95] Wilson Dizard, "Cybersecurity Plans Wait for Dhs to Complete its Evaluation of Threats," *Government Computer News*, July 25, 2005, vol. 24, no. 20.

Information and International Security, reportedly have stated that DHS does not have a robust way to detect a coordinated attack against the critical infrastructure.[96]

Security vulnerabilities found in the Internet and in critical infrastructure computer systems are widely publicized. Many experts are concerned that private sector cyber security firms do not notify DHS or their customers immediately upon recognition of a potentially serious Internet security vulnerability. If hackers become aware of this vulnerability, observers speculate that these individuals could disable portions of the Internet, or successfully disrupt selected portions of the United States or international critical infrastructure. This raises the following questions:

- Should vendors of computer products be required to quickly report all serious, newly discovered product vulnerabilities to DHS?
- Should computer service providers or businesses be required to report to DHS any major security vulnerabilities that have been newly exploited by cybercriminals?
- Should there be penalties if an organization has a poor security policy that contributes to a major loss of sensitive information?

Some actions are underway that Congress may consider.[97] For example, on September 30, 2005, an interim rule was issued by the Federal Acquisition Regulations Council, outlining several new steps acquisition workers must take to ensure IT security is incorporated into all federal purchases. Under this interim rule, government contracting officers must include additional cybersecurity rules in their acquisition planning, which will require vendors to improve computer security for the IT products and services they supply to the federal government.[98]

Experts now believe that terrorist collaborate with organized crime networks in the Middle East for international smuggling of arms and illegal drugs. Criminal drug traffickers can provide terrorists with access to computer specialists with high-level technical skills. What are the pro's and con's of linking counterterrorism efforts more closely to the efforts of agencies that counter drug trafficking?

Should the counterterrorism efforts be linked more closely with international efforts to prevent cybercrime? What are effective ways to encourage more international cooperation for identifying which activities should be labeled as cybercrime, and for punishing those who operate as cybercriminals?

---

[96] Grant Gross, *Senators Call on DHS to Improve Cybersecurity Efforts*, Symantec, at [http://enterprisesecurity.symantec.com/publicsector/article.cfm?articleid=5862&EID=0].

[97] See National Institute of Standards and Technology website for Federal Agency Security Practices, at [http://csrc.nist.gov/fasp/].

[98] Jason Miller, "IT Security Requirements Now Part of the FAR," *Government Computer News*, September 30, 2005, at [http://www.gcn.com/vol1_no1/daily-updates/37162-1.html]. *Federal Register*, September 30, 2005, vol. 70, no. 189, pp. 57449-57452.

Security experts have reportedly stated that, although U.S. military networks are relatively secure, many of those networks remain highly dependent on the civilian communications infrastructure.[99] Should DOD collaborate more closely with DHS for new technologies to strengthen the computer security of civilian agencies and infrastructure?

Trends for cybercrime indicate that computer attacks could increase in number, speed, and sophistication. Will future unknown computer vulnerabilities and sophisticated attacks allow terrorist to launch an effective cyberattack that might overwhelm the ability of civilian agencies to respond effectively? Could a new approach to computer security reduce vulnerabilities? An example of a new approach to improve computer security for computer systems and the Internet might include development and refinement of quantum methods for unbreakable cryptography.[100] However, new approaches to computer security could also lead to the emergence of new threats directed against new vulnerabilities. For example, the proliferation and use of commercial products with unbreakable cryptography could seriously undermine the ability of law enforcement to perform critical missions such as protecting against threats posed by terrorists, organized crime, and foreign intelligence agents.

Related Legislation

The following bills are related to improving national computer security, or the prevention of cybercrime:

H.R. 1. H.R. 1, "Implementing the 9/11 Commission Recommendations Act of 2007," was referred to the Senate Committee on Homeland Security and Governmental Affairs on January 9, 2007. The DHS Secretary shall evaluate and annually prioritize all pending applications for covered grants based upon the degree to which they would lessen the threat to the critical infrastructure, including, but not limited to, cyber threats. Evaluation and prioritization shall be based upon the risk assessment by the Office of Intelligence Analysis and the Office of Infrastructure Protection of the threats of terrorism against the United States.

---

[99] Barton Reppert, remarks made by Clifford Lau, July 26, 2005, at the Rayburn House Office Building, subsequent to a hearing by the House Science Committee.

[100] Quantum cryptography: In the microscopic world, once a system is observed, it is inevitably affected and changes into another state (Heisenberg's Uncertainty Principle). By incorporating the fact that weak light behaves as "photons" subject to this law, quantum cryptography is an unbreakable cryptography with the photons becoming the information carriers, or information cameras. Press Release, Mitsubishi Electric, 2002, [http://global.mitsubishielectric.com/news/news_releases/2002/mel0560_b.html].