Cyber Attacks: Protecting America's Security Against Digital Threats

Michael Vatis

ESDP-2002-04 **June 2002**

CITATION AND REPRODUCTION

This document appears as Discussion Paper ESDP-2002-04 of the Executive Session on Domestic Preparedness, a joint project of the Belfer Center and the Taubman Center for State and Local Government. Comments are welcome and may be directed to the author in care of the Executive Session on Domestic Preparedness.

This paper may be cited as Michael Vatis. "Cyber Attacks: Protecting America's Security against Digital Threats." ESDP Discussion Paper ESDP-2002-04, John F. Kennedy School of Government, Harvard University, June 2002.

ABOUT THE AUTHOR

Michael Vatis is the Director of the Institute for Security Technology Studies at Dartmouth College, and Director of the Institute for Information Infrastructure Protection (I3P). He is also of counsel to the law firm of Fried, Frank, Harris, Shriver and Jacobson, and was founder and Director of the National Infrastructure Protection Center.

The Executive Session on Domestic Preparedness is supported by Grant No. 1999-MU-CX-0008 awarded by the Office for State and Local Domestic Preparedness Support, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

> Information technology pervades all aspects of our daily lives.... Its presence is felt almost every moment of every day, by every American. It pervades everything from a shipment of goods, to communications, to emergency services, and the delivery of water and electricity to our homes. All of these aspects of our life depend on a complex network of critical infrastructure information systems. Protecting this infrastructure is critically important. Disrupt it, destroy it or shut it down ... and you shut down America as we know it and as we live it and as we experience it every day. We need to prevent disruptions, and when they occur, we need to make sure they are infrequent, short and manageable. This is an enormously difficult challenge.
>
> Tom Ridge, Director of Homeland Security[1]

The events of September 11, 2001, underscored the vulnerability to foreign attack of the territory of the United States itself, in a way not seen since Pearl Harbor. Since that day, the federal government, the media, and the public have been intensely focused on taking measures to protect us from similar attacks — or from even more devastating attacks involving weapons of mass destruction (WMD), such as nuclear, biological, chemical, or radiological weapons.

In addition to such physical attacks, however, America remains highly vulnerable to another form of attack: a "cyber attack" against the computer networks that are critical to our national and economic security. Attackers might target banking and financial institutions, voice communication systems, electrical infrastructures, water resources, or oil and gas infrastructures. The growing complexity and interconnectedness of these systems renders them increasingly vulnerable to attack. While a physical attack is likely to be carried out only by terrorists or hostile foreign nation-states, cyber attacks may be carried out by a wide array of adversaries, from teenage hackers and protest groups to organized crime syndicates, terrorists, and foreign nation-states. As a result, the problem is of enormous breadth and complexity. It requires that both our protective and reactive measures deal with each specific scenario, and not just the threat of an attack by terrorists.

In addition, the threat is challenging in another way:

---

[1] Transcript of Governor Ridge's October 8, 2001, comments, Office of the Press Secretary, U.S. Government, "New Counter-Terrorism and CyberSpace Security Positions Announced," October 9, 2001, <www.whitehouse.gov/news/releases/2001/10/20011009-4.html>.

This is the first time in American history that we in the federal government, alone, cannot protect our infrastructure. We can't hire an army or a police force that's large enough to protect all of America's cell phones or pagers or computer networks—not when 95% of these infrastructures are owned and operated by the private sector.[2]

Meeting the challenge thus requires an extraordinary level of public-private cooperation. Moreover, the global nature of the Internet means that cyber attacks can come from anywhere in the world, and occur with incredible speed. This requires an unprecedented ability by the government to respond quickly and to work effectively with international counterparts.

In this chapter, I explore some of the issues that make dealing with cyber attacks such a novel and difficult issue for the government and private sector alike. Next, I explore the history of the U.S. government's efforts to thwart and respond to cyber attacks. I conclude with recommendations for improving the government's ability to respond to such attacks at the federal, state, and local levels.

THE RANGE OF CYBER ATTACKERS

The volume, sophistication, and coordination of cyber attacks—and especially of politically motivated cyber attacks—are increasing. The FBI/Computer Security Institute's *2001 Computer Crime and Security Survey* reports all-time highs in the percentage of respondents who detected system penetration from the outside, denial of service attacks, employee abuse of Internet access privileges, and computer viruses.[3] During a single week in 2001, for example, approximately 1,200 U.S. sites, including those belonging to the White House and other government agencies, were subjected to distributed denial of service attacks or defaced with pro-Chinese images. Chinese hacker attacks in 2001 were able to reach such a massive scale because numerous hacker

[2] Remarks by Secretary of Commerce William M. Daley, "Release of National Plan for Information Systems Protection," January 7, 2000, <204.193.246.62/public.nsf/docs/F4EA9864FA0D39658525685F005FE880>.

[3] See Computer Security Institute, "Financial Losses Due to Internet Intrusions, Trade Secret Theft, and Other Cyber Crimes Soar," April 7, 2002, <www.gocsi.com/press/20020407.html>; FBI/Computer Security Institute, *2001 CSI/FBI Computer Crime and Security Survey* (Spring 2001).

groups used password-protected chat rooms and other technologies to coordinate the launch of a joint campaign against U.S. targets.[4] This section catalogs the spectrum of cyber attackers.

Insider Threat

The disgruntled insider is a principal perpetrator of computer crimes.[5] Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of the systems they are attacking may allow them unrestricted access in order to damage the system or to steal system data. The 1999 Computer Security Institute/FBI report noted that 55 percent of respondents reported malicious activity by insiders. There have been many convictions involving disgruntled insiders. For example, an employee used her insider knowledge and another employee's password and log-in identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1800 hours to recover and reenter the lost data.[6] In another case, a former employee of the Forbes publishing concern hacked into the company's systems using another employee's password and login identification, caused the crash of over half of the

[4] The United States is by no means the only nation suffering a growing volume of politically motivated cyber attacks. For example, the number of Indian website defacements attributed to pro-Pakistan hackers increased from 45 to over 250 in just three years. See Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, Sep. 22, 2001, <www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm>, p. 5.

[5] "The insider poses the greatest threat because they know where the most critical information is kept and how to bypass the safeguards on the system"; James Savage, deputy special agent in charge of the Secret Service's financial crimes division, quoted in Sharon Gaudin, "Study Looks to Define 'Insider Threat'," *Network World*, March 4, 2002, <www.nwfusion.com/news/2002/130577_03-04-2002.html>.

[6] See Laura DiDio, "U.S. Coast Guard Beefs Up Security After Hack," *CNN*.com, July 22, 1998 <www.cnn.com/TECH/computing/9807/22/coastguard.idg/>. She was convicted and sentenced to five months in prison and five months home detention, and was ordered to pay $35,000 in restitution.

company's computer network servers, and erased irretrievably all of the data on the crashed servers. The losses to Forbes were reportedly over $100,000.[7]

Criminal Groups

Criminal groups are increasingly using cyber intrusions, attacking systems for purposes of monetary gain. In 1999, for example, members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices and unauthorized access to a federal interest computer. This international group penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the FBI's National Crime Information Center (NCIC). The Phonemasters' activities should serve as a wake-up call for corporate security. Their methods included "dumpster diving" to gather old phone books and technical manuals for systems, which they then used to trick employees into giving up their log-in and password information. The group then used this information to break into target systems. This illustrates that "cyber crimes" are often facilitated by old-fashioned guile, such as tricking employees into giving up passwords. Good cyber security practices must therefore address personnel security and "social engineering" in addition to instituting electronic security measures.[8]

Virus Writers

Virus writers can do more damage to networks than hackers do. Based on data collected by a *Government Computer News* telephone survey on systems security, 43 percent of federal information technology managers deem viruses and other types of malicious code to be the biggest threats to their networks.[9] On average, over thirty new viruses are disseminated daily.

[7] Testimony of Michael Vatis, Senate Judiciary Committee Subcommittee on Technology and Terrorism, October 6, 1999, <kyl.senate.gov/sc_w25.htm> or <www.fbi.gov/congress/congress99/nipc10-6.htm>.

[8] Vatis testimony of October 9, 1999.

[9] Richard W. Walker, "Feds Say Virus Threats Keep Them Awake at Night," *Government Computer News*, August 20, 2001, <www.gcn.com/20_24/security/16834-1.html>.

About 50,000 viruses exist overall.[10] In 2001, the Code Red virus alone produced worldwide costs totaling $2.62 billion.[11] The proliferation of high-speed networks means that viruses propagate ever more quickly.[12] Anti-virus software and care with attachments can curtail such epidemics, but only if people use them consistently.

Foreign Intelligence Services

Foreign intelligence services have begun using cyber tools as part of their information gathering and espionage tradecraft. Between 1986 and 1989, for example, a ring of West German hackers penetrated numerous military, scientific, and industry computers in the United States, Western Europe, and Japan, stealing passwords, programs, and other information which they sold to the Soviet KGB.[13] Significantly, this was over a decade ago — ancient history in Internet years. It is clear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information.[14]

---

[10] See, e.g., Florence Olson, "The Growing Vulnerability of Campus Networks," *Chronicle of Higher Education*, March 15, 2002, reporting statements by Michael A. McRobbie, vice president for information technology at the Indiana University System.

[11] Jay Lyman, "In Search of the World's Costliest Virus," *E-Commerce Times*, February 21, 2002, <www.ecommercetimes.com/perl/story/16407.html>.

[12] The likelihood of a company experiencing a virus or worm, and the consequent costs, approximately doubled each year from 1995 to 1999 and grew approximately 15 percent per year in 2000 and 2001. See Lawrence M. Bridwell and Peter Tippett, *ICSA 7th Annual Computer Virus Prevalence Survey 2001*, 2002, <www.antivirus.com/download/whitepapers/icsa_vps2001.pdf>, p. 1.

[13] Clifford Stoll, *The Cuckoo's Egg* (New York: Pocket Books, 1989); Dorothy E. Denning, *Information Warfare and Security* (Reading, Mass.: Addison-Wesley, 1999), pp. 205–206.

[14] "There is little information in the public domain about the use of computer hacking in foreign intelligence operations. According to Peter Schweizer's book *Friendly Spies* [(Boston: Atlantic Monthly Press, 1993)], Germany initiated one such program ... in the mid-1980s.... The unit allegedly accessed

Information Warfare

Perhaps the greatest potential threat to our national security is the prospect of "information warfare" by foreign militaries against our critical infrastructures. We know that several foreign nations are already developing information warfare doctrine, programs, and capabilities for use against each other and the United States or other nations. Foreign nations are developing information warfare programs because they see that they cannot defeat the United States in a head-to-head military encounter and they believe that information operations are a way to strike at what they perceive as America's Achilles' heel, its reliance on information technology to control critical government and private-sector systems. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counter the military power of the United States.[15] During the recent conflict in Yugoslavia, hackers sympathetic to Serbia electronically "ping-attacked" NATO web servers.[16] Russian and other individuals supporting the Serbs attacked websites in NATO countries, including the United States, using virus-infected email and attempted hacks. Over one hundred entities in the United States received these emails, and several British organizations lost files and databases.[17] These attacks did not cause any disruption of the military effort, and the attacked entities quickly recovered. But such attacks are portents of much more serious attacks that foreign adversaries could attempt in future conflicts.[18]

---

computer systems in the United States, the former Soviet Union, Japan, France, Italy, and Great Britain." Denning, *Information Warfare and Security*, p. 64.

[15] See Kevin Anderson, "Cyber-Terrorists Wield Weapons of Mass Destruction," BBC News, Feb. 22, 2000, <news.bbc.co.uk/hi/english/sci/tech/specials/washington_2000/newsid_648000/648429.stm>.

[16] See Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, Sep. 22, 2001, <www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm>, pp. 7-8.

[17] Ibid.

[18] See generally John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (RAND 1997).

Some nations might respond to the U.S. campaign against terrorism by initiating information warfare campaigns. Iraq, Libya, and North Korea are potential targets of American military action that are thought to be developing information warfare capabilities. The possibility also exists that, because it is relatively easy to disguise the origin of online attacks, a nation-state not directly involved in American retaliatory action could launch cyber attacks against U.S. systems, disguising itself as another country that is the focus of the war on terrorism. The probable cyber-warfare capabilities of China, Cuba and Russia are of particular concern.[19]

Terrorists

There are reasons to expect terrorists to use cyber attacks to disrupt critical systems in order to harm targeted governments or civilian populations. Terrorists are known to use information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. For example, convicted terrorist Ramzi Yousef, the mastermind of the 1993 World Trade Center bombing, stored detailed plans to destroy U.S. airliners on encrypted files on his laptop computer.[20] Some groups have already used cyber attacks to inflict damage on their enemies' information systems. For example, a group calling itself the Internet Black Tigers conducted a successful "denial of service" attack on servers of Sri Lankan government embassies.[21] Sympathizers of the Zapatista rebels of Mexico attacked the web pages of Mexican President Ernesto Zedillo and the U.S. White House, as well as the Pentagon and the Frankfurt Stock Exchange.[22] A Canadian government report indicates that the Irish Republican Army has considered the use of information operations against British interests. There is concern that Aum Shinrikyo, which launched the deadly 1995 sarin gas attack in the Tokyo subway system, could use its expertise in computer manufacturing and Internet technology to develop cyberterrorism

[19] See Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis*, Sep. 22, 2001, <www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm>, p. 2.

[20] Denning, *Information Warfare and Security*, p. 68.

[21] Denning, *Information Warfare and Security*, p. 69.

[22] Denning, *Information Warfare and Security*, p. 73; also see David Ronfeldt, John Arquilla, Graham E. Fuller, and Melissa Fuller, *The Zapatista Social Netwar in Mexico* (Santa Monica, Calif.: RAND, 1998).

weapons for use against Japanese and U.S. interests.[23] Thus, while we have yet to see a significant instance of cyberterrorism with widespread disruption of critical infrastructures, it cannot be disregarded.[24]

Information about the cyber capabilities of Islamic fundamentalist organizations is incomplete. There are a number of hacker groups — such as "Iron Guard" — affiliated with Islamic terrorist organizations. But it remains unclear whether the Al Qaeda organization has developed information warfare capabilities.[25] As of March 2002, the organization had not engaged in substantial computer-based attacks. However, in mid-January 2002, the FBI received reports that Al Qaeda agents have probed government websites that contain information about nuclear power plants and other critical infrastructure. There are also many indications that the Al Qaeda organization makes sophisticated use of computer technology for fundraising, communications, and similar purposes. United States intelligence sources report that Al Qaeda is using the Internet to try to regroup and reorganize forces scattered by the global anti-terror campaign and the downfall of the Taliban regime.[26] The commander of U.S. ground forces in Afghanistan has reported that Al Qaeda fighters used the Web to stay in contact as they moved from cave to cave during battles with American and coalition troops in March 2002.[27]

---

[23] For further information about the Aum Shinrikyo cult, see David E. Kaplan and Andrew Marshall, *The Cult at the End of the World: The Terrifying Story of the Aum Doomsday Cult, from the Subways of Tokyo to the Nuclear Arsenals of Russia* (New York: Crown, 1996).

[24] Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism*.

[25] See Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada, *Threat Analysis: Al-Qaida Cyber Capability*, November 2, 2001.

[26] Ann Scott Tyson, "Al Qaeda: Resilient and Organized," *Christian Science Monitor*, March 7, 2000, p. 2; Ian Bruce, "Al Qaeda Using Internet in Bid to Regroup," *The Herald* (Glasgow), March 7, 2000, p. 10.

[27] Brian Williams, "Afghan Foes Used Web, Had Money to Burn, Feds Say," March 19, 2000, <www.reuters.com/news_article.jhtml?type=technologynews&StoryID=717621>.

"Hacktivism"

Recently there has been a rise in what has been dubbed "hacktivism" — politically motivated attacks on publicly accessible web pages or email servers. Groups and individuals seek to overload email servers and to hack into web sites in order to send a political message. While these attacks generally have not altered operating systems or networks, they still damage services, and by denying the public access to websites containing valuable information, they infringe on others' right to communicate. One such group, the "Electronic Disturbance Theater," promotes civil disobedience online in support of its political agenda regarding the Zapatista movement in Mexico and other issues.[28] Supporters of Kevin Mitnick, convicted of numerous computer security offenses, hacked into the Senate webpage and defaced it in May and June 1999.[29] Members of the anti-capitalism and anti-globalization movement launched denial of service attacks during the 2002 World Economic Forum in New York City.[30]Hacktivism could also be connected to national security issues. If, for example, American diplomacy regarding the war on terrorism and Middle East affairs is unsuccessful, the region could become further polarized into two camps: those that sympathize with Israel, and those that sympathize with Arab states. If the United States is consistently portrayed as allying with the former, and "us vs. them" mind frame may intensify. Pro-Arab and pro-muslim groups throughout the world could become players in a scenario in which sophisticated and sustained cyber attacks are carried out against American interests as a form of anti-American hacktivism. There is also a real danger that a wider polarization, involving groups with any grievance against the United States or its allies could ensue, potentially creating a large and diverse hostile and politically active coalition.

---

[28] Denning, *Information Warfare and Security*, p. 73.

[29] For more information about pro-Mitnick "cyber protests" (i.e. hacktivist cyber attacks), see "Feds Warn Hackers Will Be Prosecuted; Pro-Mitnick Protest Planned," CNN.com, June 2, 1999, <www.cnn.com/TECH/computing/9906/02/hunting.hackers/>.

[30] See Noah Shachtman, "Econ Forum Site Goes Down," *Wired.com*, Jan. 31, 2002, <www.wired.com/news/politics/0,1283,50159,00.html>.

"Recreational" Hackers

Virtually every day there is another report about "recreational hackers," or "crackers," who penetrate networks for the thrill of it or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill and computer knowledge, the recreational hacker can now download attack scripts and protocols from the World Wide Web and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.

These types of hacks are numerous and may appear on their face to be benign, but they can have serious consequences. A well-known 1997 example involved a juvenile who used his personal computer and modem to hack into the telephone system that served the area of Worcester, Massachusetts. The attack shut down telephone service to 600 customers in the local community. The resulting disruption affected all local police and fire 911 services as well as the ability of incoming aircraft to activate the runway lights at the Worcester airport. Telephone service was out at the airport tower for six hours.[31] The U.S. Secret Service investigation of this case also brought to light a vulnerability in 22,000 telephone switches nationwide that could be taken down with four keystrokes. Because he was a juvenile, however, the hacker was sentenced to only two years probation and 250 hours of community service, and was forced to forfeit the computer equipment used to hack into the phone system and reimburse the phone company $5,000. This case demonstrated that an attack against our critical communications hubs can have cascading effects on several infrastructures. In this case, transportation, emergency services, and telecommunications were disrupted. It also showed that widespread disruption could be caused by a single person from his or her home computer.

TYPES OF CYBER ATTACKS

Cyber attacks are computer-to-computer attacks carried out to steal, erase, or alter information, or to destroy or impede the functionality of the target computer system. These attacks typically fall into three general categories: unauthorized intrusions, in which the attacker breaks into the computer system using various hacking techniques, or an insider exceeds his or her authorized access in order to do unauthorized things to the network; destructive viruses or worms, which spread from computer to computer through email or other forms of data exchange and can cause

[31] Denning, *Information Warfare and Security*, p. 51.

the loss of functionality of parts of the network; and denial of service (DOS) attacks, using any of several techniques to bombard the target computer with communications and overload it, thereby hampering its functioning.[32] In this section, I describe the kinds of attacks that politically motivated cyber attackers are especially likely to perpetrate against the United States.

Web Defacements and Semantic Attacks

Website defacements are the most common form of politically motivated cyber attack. The most serious consequences of web defacements result from "semantic attacks," which change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated.

Domain Name Server (DNS) Attacks

Computers connected to the Internet communicate with one another using numerical Internet Protocol (IP) addresses.[33] Computers consult domain name servers (DNS) to map the name of a website (e.g. cnn.com) to its numerical address (64.12.50.153). If the DNS provides an incorrect numerical address for the desired website, then the user will be connected to the incorrect server, often without the user's knowledge. A DNS attack can thus be used to disseminate false information or to block access to the original website.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service attacks subject web and email servers to overwhelming numbers of communications from other computers. The high volume of communications can slow or crash the target system. Hackers often multiply the force of their DDoS attacks by using malicious code

[32] See Michael Vatis, *International Cyber Security Cooperation: Informal Bilateral Models* (Washington, D.C.: Center for Strategic and International Studies [CSIS], 2002). For a thorough enumeration of types of computer security incidents, see Thomas A. Longstaff, et al., "Security of the Internet," CERT Coordination Center, <www.cert.org/encyc_article/tocencyc.html#TypesInc>.

[33] An IP address is a number that identifies the sender or receiver of information sent across the Internet. For a more detailed explanation of IP addresses, see <whatis.techtarget.com/definition/0,289893,sid9_gci212381,00.html>.

to take control of other users' machines and using these "zombie" machines to send additional communications to targeted servers.

Malicious Code

Worms, viruses, and Trojan horses are types of malicious code.[34] The vulnerabilities that worms and viruses exploit are usually well known to system administrators and can be remedied, but nevertheless they often go uncorrected on so many systems that worms and viruses are able to cause major problems in the information infrastructure. If maximum destruction is a hostile adversary's goal, malicious code offers a cost-effective way to significantly disrupt the U.S. information infrastructure.[35]

Exploitation of Routing Vulnerabilities

Routers are the "air traffic controllers" of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing disruptions from malicious activity have been rare, but the lack of diversity in router operating systems leaves open the possibility of a massive routing attack. The malicious reprogramming of even one router could lead to errors throughout the Internet.

Compound Attacks

By combining methods, hackers could launch an even more destructive attack. Another strategy might be to magnify the destructiveness of a physical attack by launching coordinated cyber

[34] A virus is a program or piece of code that is loaded onto a computer without the authorized user's knowledge, and runs against the user's wishes. Viruses can replicate themselves. Even a simple virus is dangerous because it can use all available memory and bring the system to a halt; even more dangerous are those capable of transmitting themselves across networks and bypassing security systems. A worm is a type of virus that can replicate itself and use memory, but cannot attach itself to other programs. A Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves, but they can still be destructive.

[35] See Institute for Security Technology Studies, *Cyber Attacks During the War on Terrorism: A Predictive Analysis,* Sep. 22, 2001, <www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm>, p. 12.

attacks. For example, attackers might set off a bomb in a heavily populated building and simultaneously disable the community's "911" emergency telephone system.

Even when terrorists do not deliberately coordinate cyber attacks and physical attacks, a direct relationship persists between them. Political conflict usually leads to higher levels of cyber attacks. For example, the April 1, 2001 mid-air collision between an American surveillance plane and a Chinese fighter aircraft, and the February 2000 air strikes by Israel against Hezbollah sites in Lebanon, correlated with spikes in the number of cyber attacks against the involved parties.[36] However, during the first six months of the U.S. campaign against terrorism, the United States does not appear to have experienced higher than normal levels of malicious online activity, perhaps due to an upsurge of American patriotism and foreign sympathy, or to the high level of alert of U.S. "cybercops" and system administrators. However, these mitigating factors could well be only temporary.

Politically-motivated hackers will seek to attack high-value targets, including networks, servers, or routers whose disruption would have symbolic, financial, political or tactical consequences. Assaults during the second Palestinian *intifada* on Israeli banking and telecommunications websites should serve as a warning.[37] The Code Red worm, which targeted the White House web site, reminds us that politically motivated cyber attackers may attempt to disable symbols of the American government.[38]

THE INTERNATIONAL COMPONENT OF CYBER ATTACKS

Cyber attackers are able to take advantage of the complications associated with cross-border law enforcement. A typical cyber investigation can involve target sites in multiple states or countries, and can require tracing an evidentiary trail that crosses numerous state and international

[36] ISTS, *Cyber Attacks During the War on Terrorism*, 9.

[37] The "cyber jihad" undertaken by hackers supporting the second Palestinian intifada had specific stages during which Israeli financial institutions and Israeli telecommunications firms, respectively, were targeted. ISTS, *Cyber Attacks During the War on Terrorism*, 7.

[38] ISTS, *Cyber Attacks During the War on Terrorism*, 10.

boundaries.[39] Even intrusions into U.S. systems by a perpetrator operating within the United States may require international investigative activity, because the attack is routed through Internet service providers and computer networks located outside the United States. When evidence is located within the United States, law enforcement authorities can subpoena records, conduct electronic surveillance, execute search warrants, and seize and examine evidence. However, U.S. authorities can do none of those things overseas; instead, they must depend on the assistance of local authorities. This means that effective international cooperation is essential to cyber crime investigations.

International cyber investigations pose special problems. First, the transient or perishable nature of digital evidence requires more expeditious response than has traditionally been possible in international matters. Internet service providers and system administrators of networks are always looking to discard unneeded information in order to save storage costs; thus if digital evidence, such as historical transaction data or "log" information recording certain network activity, is not specifically located and preserved quickly, it might be lost for good by the time formal procedures are completed. Hackers might even go back into a network and erase their digital trail if they suspect that law enforcement is onto them. As a result, the delays typically associated with cross-border law enforcement are especially likely to impede an international cyber investigation.

Second, many foreign criminal justice systems are poorly prepared to respond to cyber crimes. While the situation has improved markedly in recent years, some countries still lack substantive criminal laws that specifically cover computer crimes; as a result, these countries may lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist the United States when it seeks evidence located in those countries. The quickly evolving technological aspects of these investigations can exceed the capabilities of local police forces in some countries. Since no country to date has been willing to allow another country to conduct a unilateral investigation on its own soil, either physically or virtually, the limits on the technical savvy of foreign law enforcement officials can seriously inhibit American cyber investigations.

---

[39] It has been estimated that seventy percent of attacks on computer systems worldwide originate outside the United States. Ranae Merle, "Computer Attacks on Companies Up Sharply," *Washington Post*, Jan. 28, 2002.

Finally, there are few formal mechanisms for international cooperation in cyber investigations. Formal bilateral arrangements for information sharing, generally embodied in "Mutual Legal Assistance in Criminal Matters Treaties" (MLATs), do not exist between all of the countries that might need to cooperate on a cyber crime investigation. The United States has MLATs in force with only 19 countries (with another 15 signed but not yet ratified).[40] Furthermore, many MLATs do not cover computer crimes (either specifically or through broadly applicable general terms), and their procedures are typically time-consuming and burdensome. Multilateral conventions (informal as well as formal) have proven difficult for a number of reasons. One significant reason is that the growth of computer crime has affected different countries at different rates, meaning that many countries have not yet (or until recently) had to face the problem in a serious way. Countries that have not adopted a rigorous internal approach to the problem of computer crime are ill-prepared to enter multilateral negotiations. A second reason is the difficulty of distinguishing some "cyber crime" from "information warfare" and cyber espionage. If a foreign intelligence agency committed an intrusion, then that country's government is unlikely to render effective assistance to U.S. investigators.

The effectiveness of informal multilateral initiatives such as the G8 Subgroup on High-Tech Crime[41] and informal bilateral efforts such as the collaboration between the NIPC and Israeli law enforcement on the Solar Sunrise investigation[42] partly compensates for the weakness of formal

[40] See U.S. State Department, Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and Other Agreements, at <www.travel.state.gov/mlat.html>.

[41] See Vatis, *International Cyber Security Cooperation.*

[42] In February 1998, there were attacks on approximately half a dozen military networks and hundreds Domain Name Servers. The attack was initially traced to Abu Dhabi in the United Arab Emirates, but a multi-agency investigation led by NIPC, code-named SOLAR SUNRISE, soon determined that it was the work of two California teenagers, assisted by an Israeli citizen. For more information on the Solar Sunrise incident and the NIPC's role in international investigations, see Testimony of Michael Vatis, House Committee on Government Affairs, Subcommittee on Government Management, Information, and Technology, July 26, 2000, <www.fbi.gov/congress/congress00/vatis072600.htm>.

mechanisms. However, the expansion of formal—and informal—mechanisms is vital to improving U.S. cybersecurity.[43]

THE FEDERAL RESPONSE TO CYBER ATTACKS

The federal government has for decades devoted substantial resources to building America's information infrastructure. A researcher at a government-funded think tank developed the precursor to the Internet's essential packet switching technology around 1960, in a research project aimed at providing the U.S. military with a communications system that could survive nuclear attack.[44] The Internet itself grew out of ARPANET, a Defense Department program to develop a communication network to link scientists working on DoD-funded research projects.[45] Government efforts to protect that infrastructure, however, are much more recent.

Early Efforts at Information Infrastructure Protection

The federal government began focusing on cyber attacks in earnest during the mid-1990s.[46] Motivated by the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the Clinton administration in late 1995 convened the Critical Infrastructure Working Group (CIWG) to assess the vulnerabilities of the nation's "critical infrastructures" to attack, and to make

[43] See Vatis, *International Cyber Security Cooperation*.

[44] See Janet Abbate, *Inventing the Internet* (Cambridge, Mass.: MIT Press, 1999), pp. 8, 11. The researcher was Paul Baran of the RAND Corporation.

[45] Abbate, *Inventing the Internet*, pp. 43–44.

[46] The National Security Agency, the National Institute for Standards and Technology (NIST) at the Department of Commerce, and some other agencies have worked on computer security issues for many years. But government-wide policymaking to address the vulnerabilities of, and threats to, vital computer networks and the critical infrastructures that rely on them did not begin until the 1990s, with the rapid growth of the Internet.

recommendations to the president on how to protect them.[47] The CIWG defined as "critical infrastructures" those systems and facilities comprising the institutions and industries that provide a continual flow of goods and services essential to the defense and economic security of the United States, the functioning of government at all levels, and the well-being of society as a whole.[48] Moreover, it warned that critical infrastructures were vulnerable not only to physical attacks like the one seen in Oklahoma City, but also to "cyber attacks" against the computer networks that are used to control the delivery of vital services. In its January 1996 report, the CIWG recommended the creation of a full-time commission, comprising representatives from both government and private industry, to develop a national strategy for protecting the critical infrastructures, and also an interim task force to coordinate the government's existing capabilities for responding to infrastructure attacks.[49]

Based on the CIWG's recommendations, President Clinton signed Executive Order 13010 in July 1996, creating the President's Commission on Critical Infrastructure Protection (PCCIP) to study the problem in depth and to develop proposed solutions.[50] The Executive Order also established,

---

[47] The Critical Infrastructure Working Group (CIWG), which I led on behalf of Deputy Attorney General Jamie Gorelick, comprised representatives from many federal agencies, including the Departments of Justice and Defense, the FBI, and the CIA, as well as various parts of the Executive Office of the President.

[48] Presidential Decision Directive 63 would subsequently define critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government." The eight critical infrastructure sectors are telecommunications, electric power, transportation, oil and gas delivery and storage, banking and finance, water, emergency services, and critical government services.

[49] Office of the Attorney General, Memorandum on Critical Infrastructure Security, March 14, 1996, <www.fas.org/sgp/othergov/munromem.htm>, summarizes the work of the CIWG. Senate Governmental Affairs Permanent Subcommittee on Investigation, "Hearing Report: Security in Cyberspace," June 16, 1996, <www.nist.gov/hearings/1996/secycyb.htm>, summarizes a Senate hearing on the CIWG's recommendations and related matters.

[50] Executive Order No. 13,010, 61 Fed. Reg. 37,345 (July 17, 1996), <www.access.gpo.gov/su_docs/aces/aces140.html>.

at the Department of Justice, the Infrastructure Protection Task Force (IPTF). This interagency body, led by the FBI, was designed to facilitate the coordination of existing infrastructure protection efforts in the interim period, while the PCCIP conducted its analysis and developed long-term recommendations.[51]

PDD 62 and 63

The PCCIP's final report became the basis for Presidential Decision Directive (PDD) 63, which outlined the federal government's approach to critical infrastructure protection.[52] Signed by President Clinton on May 22, 1998, it created intra-governmental and public-private cooperative structures to address policymaking, preventive measures, and operational matters.

PDD 62, which set forth the government's counterterrorism policy, was signed the same day. It created, within the National Security Council staff, the position of National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism to oversee the government's activities and ensure implementation of PDD 62, PDD 63, and PDD 39, which had assigned responsibility to act as lead agency for counterterrorism to the Department of Justice. Richard Clarke, a senior NSC staffer responsible for counterterrorism, was appointed to the new post.

PDD 63 also created the Critical Infrastructure Assurance Office (CIAO), located in the Commerce Department, which supports the National Coordinator in outreach and policy planning, including the development of the National Plan for Information Systems Protection ("National Plan"), which was released in January 2000. The National Plan outlines the steps the federal government will take to protect its own information assets and to develop a public-private

[51] See Testimony of Michael Vatis before the Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Government Information, June 10, 1998, <www.fas.org/irp/congress/1998_hr/98061101_ppo.html>, for a brief history of these recommendations.

[52] See Critical Infrastructure Assurance Office, "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 1998, <www.ciao.gov/CIAO_Document_Library/paper598.htm>. PDD 62 and PDD 63 are summarized in a White House press release dated May 22, 1998, at <www.info-sec.com/ciao/6263summary.html>.

partnership dedicated to defending the nation's critical infrastructures. Its three objectives are summed up as "Prepare and Prevent," "Detect and Respond," "Build Strong Foundations."[53]

PDD 63 introduced three mechanisms for improving public-private cooperation. It designated "lead agencies" to work with private industry in each infrastructure sector to address critical infrastructure problems, develop parts of the national plan, and engage in education and vulnerability awareness activities with each industry sector.[54] In addition, PDD 63 encouraged the

[53] "Prepare and Prevent" means to prevent attacks against critical information networks and to "harden" these networks so that they can remain effective in the face of attacks. "Detect and Respond" requires the ability to detect and assess an attack quickly and then to contain the attack, recover from it, and reconstitute affected systems. "Build Strong Foundations" refers to the need to cultivate human, organizational, and legal resources that will make American society better able to accomplish the first two objectives. National Plan, Executive Summary, p. xi. The plan outlines ten programs for achieving these objectives: (1) identify critical infrastructure assets and shared interdependencies and address vulnerabilities; (2) detect attacks and unauthorized intrusions; (3) develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law; (4) share attack warnings and information in a timely manner; (5) create capabilities for response, reconstitution and recovery; (6) enhance research and development in support of programs 1–5; (7) train and employ adequate numbers of information security specialists; (8) outreach to make Americans aware of the need for improved cyber-security; (9) adopt legislation and appropriations in support of programs 1-8; and (10) in every step and component of the plan, ensure the full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data. National Plan, Executive Summary, pp. xi–xii.

[54] PDD 63 designates lead agencies as follows: the Commerce Department for information and communications; the Treasury Department for banking and finance; the Environmental Protection Agency for water supply; the Department of Transportation for aviation, highways, mass transit, pipelines, rail, waterborne commerce; the Justice Department / FBI for emergency law enforcement services; the Federal Emergency Management Agency for emergency fire service and continuity of government; and the Department of Health and Human Services for public health services. It specifies lead agencies for special

creation of one or more Information Sharing and Analysis Centers (ISACs) in each sector. These centers, located in the private sector, are intended to gather, analyze, sanitize, and disseminate private-sector information to industry and government. At least a segment of each of the eight critical infrastructure sectors identified by the federal government has created or is developing an ISAC.[55] PDD 63 also created the National Infrastructure Advisory Council (NIAC), a panel of industry CEOs and other private-sector experts, to promote cooperation between businesses and government on computer security issues.

On operational matters, the Directive formally recognized the creation of the National Infrastructure Protection Center (NIPC), an inter-agency center housed at the FBI that had been created by Attorney General Janet Reno in February 1998 (in consultation with the Secretary of Defense, the Director of the FBI, and other officials). NIPC has operational responsibility for dealing with cyber attacks on critical U.S. infrastructures.[56] The NIPC is the focal point for information-gathering, threat assessment, warning, and investigation. Because viruses and other malicious codes spread so quickly and because digital evidence is fleeting, the NIPC is structured to perform these functions very rapidly.

For example, less than two hours after it first received word of the ILOVEYOU virus in May 2000, NIPC had verified this initial report, assessed the virus, and contacted the Federal

---

functions: the State Department for foreign affairs; the CIA for intelligence; the Defense Department for national defense; and Justice/FBI for law enforcement and internal security.

[55] See National Infrastructure Protection Center (NIPC), *Highlights,* April 2001, <www.nipc.gov/publications/highlights/2001/highlight-01-05.htm>; Willard S. Evans, Jr., "Security: Protecting Critical Infrastructures by Sharing Information," *Energy IT*, January/February 2002, <www.platts.com/infotech/issues/0201/0201eit_security.shtml>; Energy ISAC, <www.energyisac.com/>; Association of Metropolitan Water Agencies, *Information Sharing and Analysis Center: Planning for the Water ISAC Implementation*, <www.amwa.net/isac/waterisac.html>; National Coordinating Center for Telecommunications, Telecommunications ISAC Information Portal, <www.ncs.gov/InformationPortal/portal.html>.

[56] The NIPC performs the lead agency and special functions roles specified for Justice/FBI in PDD 63.

Computer Incident Response Center (FedCIRC) and the Computer Emergency Response Team Coordination Center (CERT/CC at Carnegie Mellon University), the institutions responsible for assisting government and private sector system administrators.[57] The FBI investigation of the virus, coordinated and supported by the NIPC, also proceeded at high speed. Within a day of the virus's spread, the FBI had contacted authorities in the Philippines, where FBI investigators collaborated with the Philippine National Bureau of Investigation (NBI), whose officers had been trained as part of the NIPC international outreach program. Within a few days more, the NBI officers had arrested a suspect.[58]

The NIPC's status as an inter-agency center housed at the FBI, as well as its strong ties with the private sector and with state and local law enforcement, are essential to its ability to carry out its operational functions rapidly. The FBI's legal authority to conduct criminal investigations makes it able to gather and retain the information necessary to determine the source, nature, and scope of an incident.[59] But the broad scope of cyber threats—including foreign espionage, information warfare, and cyberterrorism—frequently implicates the portfolio and expertise of the Department of Defense, the intelligence community, infrastructure-focused civilian agencies such as the Departments of Energy and Transportation, and/or state and local law enforcement. The key role

[57] The Computer Emergency Response Team Coordinating Center (CERT/CC) is a center of Internet security expertise at the Software Engineering Institute <www.sei.cmu.edu>, a federally funded research and development center operated by Carnegie Mellon University <http://www.cmu.edu>.

[58] "Police Arrest 'ILOVEYOU' Suspect," *ZDNet UK*, May 8, 2002, <news.zdnet.co.uk/story/0,,s2078816,00.html>. The suspect was subsequently released—in part because Philippine law did not specifically cover computer crime. The absence of a computer crime law made it very unlikely that prosecutors could obtain a conviction.

[59] See Statement of Michael A. Vatis before the Senate Committee on Judiciary, May 25, 2000, <judiciary.senate.gov/oldsite/52520mav.htm>.

of businesses in maintaining and upgrading critical infrastructures makes NIPC outreach efforts to the private sector a crucial tool for mitigating the consequences of cyber attacks.[60]

Bush Administration Policy

The Bush administration plans to detail its approach to information systems protection in a new national plan to be released in the summer of 2002.[61] It has demonstrated its awareness of the severity of the digital threat by proposing substantial increases in federal spending on computer and network security from $2.7 billion in fiscal year 2002 to $4.2 billion in fiscal year 2003.[62]

---

[60] Among these outreach efforts are the Key Asset Initiative and InfraGard. The Key Asset Initiative (KAI) is a program aimed at creating a professional relationship between the FBI and identified Key Assets, on a local level. A Key Asset is defined as an organization, group of organizations, system, or groups of systems, or physical plant of which the loss would have widespread and dire economic or social impact. <www.nipc.gov/infosharing/infosharing2.htm>. InfraGard is an information sharing and analysis effort that is a cooperative undertaking between the U.S. government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. <www.infragard.net/>.

[61] Dan Verton, "Schmidt Lays Out Cyberprotection Board Agenda," *ComputerWorld*, March 13, 2002, at <www.computerworld.com/storyba/0,4125,NAV47_STO69066,00.html>. The Bush plan, which will supersede the National Plan released by the Clinton administration in 2000, will reportedly be based largely on input from private companies.

[62] See Matthew Fordahl, "High-Tech Security Czar Warns Against Cyber Complacency," February 20, 2002, <www.washtech.com/news/regulation/15251-1.html>. Recent increases in the Bush administration's cybersecurity budget have not been wholly deliberate: the 2000 Government Information Security and Reform Act requires agencies to report their cybersecurity efforts to the Office of Management and Budget (OMB). When OMB deems that a budget does not adequately address security problems, it can either send the budget back to the agency or shift money from other spending categories to cybersecurity. See Joshua

Mark Forman, associate director for information technology and e-government at the Office of Management and Budget, has stated that President Bush plans to ask for a 15.5 percent increase in information technology spending in his fiscal 2003 budget, the biggest such increase in at least five years.[63] The Bush administration has identified cybersecurity education and research and development as special budgetary priorities.[64]

The substantive content of Bush administration cybersecurity policy has been similar to that of the Clinton administration; it continues to emphasize the crucial importance of public-private partnerships, recognizing that the U.S. government currently lacks the legal authority and the capability to single-handedly defend the nation's critical infrastructures. Like its predecessor, the Bush administration is acutely conscious that the private sector owns and operates most of the nation's essential networks and employs many of the field's leading technical experts.[65]

Dean and Shane Harris, "President Calls for Major Technology Spending Increase," February 1, 2002, <www.govexec.com/dailyfed/0202/020102h1.htm>.

[63] Dean and Harris, "President Calls for Major Technology Spending Increase."

[64] Carolyn Duffy Marsan, "Security Chief Details U.S. Cybersecurity Plans," *InfoWorld*, March 12, 2002, <www.infoworld.com/articles/hn/xml/02/03/12/020312hnbush.xml>; Verton, "Schmidt Lays Out Cyberprotection Board Agenda"; Maureen Sirhal, "White House Official Outlines Cybersecurity Initiatives," January 25, 2002, <www.govexec.com/dailyfed/0102/012502td1.htm>. Among other steps, the Bush administration plans to expand the Clinton administration's Cybercorps (Federal Cyber Services) program, which provides scholarships to students of information assurance who agree to work full-time for a federal agency upon graduation. Colleen O'Hara, "NSF Launches Grants for Cybercorps," *Federal Computer Week*, April 19, 2000, <www.fcw.com/fcw/articles/2000/0417/web-cyber-04-19-00.asp>.

[65] Paul Kurtz, director of Critical Infrastructure Protection for the White House, has acknowledged that, "First and foremost, we must form a partnership with the private sector." Sirhal, "White House Official Outlines Cybersecurity Initiatives." Kurtz also noted that the current White House cybersecurity team was continuing a Clinton administration initiative to ensure that security is built into the next generation of computer systems. Ibid. Bara Vaida, "Clarke Presses Private Sector to Protect Against Cyber Attacks," February 14, 2002, <www.govexec.com/dailyfed/0202/021402td1.htm>, reports that Richard Clarke,

The cybersecurity policies of both administrations have focused on building partnerships between business and government and also on promoting cooperation between government agencies and between businesses. The Clinton administration located operational responsibility for thwarting digital threats in an inter-agency center (the NIPC) and encouraged competitors to share information (as members of the same ISAC). President Bush established the President's Critical Infrastructure Protection Board (PCIPB) to coordinate federal infrastructure protection efforts.[66] He moved the PCIPB, the NIPC, and the CIAO into the same building.[67] His administration has also encouraged companies to share information about cyber attacks, and supported changes in the Freedom of Information Act and antitrust enforcement that would remove legal impediments to such information sharing.[68]

On the whole, both administrations have eschewed regulations that would require companies to take security measures.[69] Two exceptions are the Gramm Leach Bliley Act,[70] which imposes

---

Special Advisor to the President for Cyberspace Security, has repeatedly stated that convincing private companies to invest in computer security is a top administration priority.

[66] Thomas R. Temin, "Bush Establishes Cybersecurity Board," *Government Computer News*, October 22, 2001, <www.gcn.com/20_31/news/17361-1.html>.

[67] See Diane Frank, "Cybersecurity Center Takes Shape," *Federal Computer Week*, Feb. 18, 2002, < http://www.fcw.com/fcw/articles/2002/0218/news-cyber-02-18-02.asp>.

[68] See Sirhal, "White House Official Outlines Cybersecurity Initiatives."

[69] Howard Schmidt, vice chairman of President Bush's PCIPB and former chief security officer for Microsoft, said, "It's got to be voluntary because if we don't work in a spirit of cooperation and trust, we are shooting ourselves in the foot at the outset." Molly M. Peterson, "Public-Private Partnerships Called Key to Cybersecurity," March 12, 2002, <www.govexec.com/dailyfed/0302/031202td2.htm>. Marsan, "Security Chief Details U.S. Cybersecurity Plans," reports that the Bush administration is committed to a voluntary approach emphasizing information sharing and best practices rather than new regulation.

[70] Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999). Section 6801 of the Act requires that financial institutions protect nonpublic personal information by

minimum security requirements on financial service companies, and the Health Insurance Portability and Accountability Act,[71] which imposes similar minimum security requirements on health care providers. These Acts were passed out of a concern for protecting the privacy of customer and patient data stored electronically, more than concern for security of the computer network and infrastructures. However, if the number and severity of cyber attacks continue to increase, the GLB and HIPAA regulations could provide a model for other industry sectors to address their concern for computer network security.

RECOMMENDATIONS

In this section, I outline recommendations that must be a priority for both government and the private sector to protect critical infrastructure against digital threats.

Expand Cyber Security Research and Development

The U.S. government must expand its support for the development of technologies that build security into new information technologies "from the ground up." The Internet itself was never designed with security as a primary consideration, and therefore vulnerabilities are embedded in the very foundation of our information infrastructure. Much work is currently underway in the private sector to develop new virus detection software, "firewalls," and the like. But commercial research is largely focused on existing threats and near-term profit-making developments. What

---

adopting a privacy obligation policy and sufficient safeguards to ensure the security and confidentiality of customer records and information.

[71] Health Insurance Portability and Accountability Act of 1996, Pub. L No. 104-191, 110 Stat. 1988. The Act provides that if Congress did not pass comprehensive privacy legislation by August 21, 1999, the Department of Health and Human Services (HHS) was required to promulgate appropriate privacy regulations. The final HHS Privacy Rule, which took effect on April 14, 2000, addresses the obligation of health care providers and health plans to protect medical information. It gives patients greater access to their own medical records and more control over how their personal health information is used. See Health Care Financing Administration, *Standards for Privacy of Individually Identifiable Health Information: The HIPAA Privacy Rule*, <www.hcfa.gov/medicaid/hipaa/adminsim/privacy.htm>.

remains sorely needed is research that can look at the mid- and long-term threats and develop secure, next-generation networks.

To obtain the maximum benefit from cybersecurity research and development, however, requires more than just increased funding. The government must also identify priorities and gaps in existing research. What is needed is a prioritized national agenda for information assurance research and development.[72] In 2001, Congress funded an institution — the Institute for Information Infrastructure Protection (I3P) — to compile such an agenda, compare the priorities identified therein with existing research, and either fund or carry out R&D to fill the gaps.[73] The success—and continued funding—of this enterprise is vital to the long-term security of the nation's information infrastructure.

The Nation Must Be on High Cyber Alert During Periods of Conflict

During periods of military conflict and international tension, U.S. government officials and system administrators should be on high alert for the warning signs of impending hostile cyber activity. Cyber attacks may accompany physical attacks; for example, cyber attacks followed NATO intervention in Kosovo during the spring of 2000, the April 2001 mid-air collision

[72] See, e.g., Institute for Defense Analysis (IDA), *A National R&D Institute for Information Infrastructure Protection (I3P)* (Washington, D.C.: IDA, 2000); Office of Science and Technology Policy (OSTP), "White Paper on the Institute for Information Infrastructure Protection" (Washington, D.C.: OSTP, July 11, 2000).

[73] The Institute for Information Infrastructure Protection ("I3P") was established at Dartmouth College's Institute for Security Technology Studies; it is a consortium of leading cybersecurity and information infrastructure protection (IIP) centers that is developing a national research agenda to be published by early 2003. The I3P website is located at <www.thei3p.org>. Documents supporting the creation of an I3P include IDA, *A National R&D Institute for Information Infrastructure Protection (I3P)*; and OSTP, "White Paper on the Institute for Information Infrastructure Protection." Also recommending continuous funding for information security research and development to keep pace with cyber attackers is Center for Strategic and International Studies, *Defending America — Redefining the Conceptual Borders of Homeland Defense — Critical Infrastructure Protection and Information Warfare* (Washington, D.C.: CSIS, 2000).

between an American surveillance plane and a Chinese fighter aircraft, and other recent international incidents. Similar attacks might ensue as the United States carries out campaigns against terrorist groups and state sponsors. To prepare for periods of high alert, government officials should implement systematic and routine risk assessments of information infrastructures, oversee development of an incident management plan, and ensure that law enforcement contact information is readily available in case of attack.

Identify and Follow Standard "Best Practices" for Computer and Physical Security

Agency heads, CEOs, and other leaders must ensure that their organizations' standard operating procedures incorporate existing best practices for security.

Consider Both Regulatory and Incentive-based Approaches to Improving Private Sector Cybersecurity

The Bush administration recognizes that the vulnerability of private sector computer networks is a threat to national security. The interconnectedness of nodes in information networks also means that computer security has substantial externalities. The existence of large externalities in an area with important national security implications is a powerful argument for government intervention. The government should consider the appropriateness of regulations requiring companies to take security measures. It should also examine approaches that would create market incentives for investment in infrastructure protection. Such measures could include reform of tort laws to expand liability for security breaches, regulation that would tie favorable insurance rates to compliance with industry standards and best practices, and the expansion of relevant subsidies and tax breaks.

Secure Critical Information Assets

Any host or network component, the loss of whose services might result in serious communications failure or financial loss, should be considered a critical information asset. While cost considerations make extraordinary protection of all systems impractical, measures for securing the most critical systems should be implemented wherever possible. These measures can include backing up data and storing copies off-site, building redundancies into key communications systems, and decoupling systems so that failures are more easily contained within a part of the network or infrastructure. All of an organization's measures to secure critical infrastructure assets should be clearly explained to its members in an enforceable security policy.

Expand Existing Institutions that Perform Operational Warning and Response Functions

The severity of the digital threat has grown much more rapidly than the budgets of the agencies charged with managing it, including the NIPC, FedCIRC, and CERT-CC. The NIPC, for example, received just $27 million in FY 2002; meanwhile the number of cybersecurity incidents and the number of computer security vulnerabilities more than doubled in 2001.[74] The estimated worldwide cost in 2001 of attacks using malicious code was $13.2 billion.[75] U.S. investments in mechanisms that gather information, assess threats, provide warnings, defeat attacks, investigate incidents and assist recovery have not kept pace. Institutions such as the NIPC, FedCIRC and CERT-CC need additional resources.

Help State and Local Governments Develop More Sophisticated Cybersecurity Capabilities

State and local government employees will be among the first to respond to any terrorist attack in the United States. After September 11, this assertion is self-evident in the case of physical attacks, and although it may be less obvious in the online context, it is equally true. It is therefore imperative to empower state and local governments to help residents and businesses respond to computer security incidents. At the same time, state and local governments must improve the security of their own computer networks. A physical attack would have much more severe consequences if terrorists used a cyber attack to disable a jurisdiction's emergency response system or other critical infrastructures. Federal agencies should help their state and local counterparts develop the capacity to prevent, prepare for, identify, and recover from the cyber component of potential compound attacks.

Develop Legal Mechanisms and Relationships to Facilitate Cross-Border Investigation and Enforcement

As it works to improve cross-border responses to cyber attacks, the United States should focus on expanding informal bilateral and formal multilateral cooperative arrangements. NIPC has established programs that strengthen the "trust networks" essential to informal bilateral cooperation: it sponsors classes for foreign law enforcement; develops information-sharing

[74] CERT-CC, "CERT/CC Statistics 1988-2001," <www.cert.org/stats/cert_stats.html>.

[75] *Computer Economics, 2001 Economic Impact of Malicious Code Attacks*, January 2, 2002, <www.computereconomics.com/cei/press/pr92101.html>.

relationships with foreign watch centers; and invites other countries to send liaison representatives to the NIPC. Such practices should be expanded. Inevitably, however, the United States will find that a cyber attack has originated from or passed through a country outside of our trust network. It is therefore important that the United States support formal multilateral agreements that will oblige all parties to help one another respond to cyber attacks. In particular, the federal government should conclude international agreements providing that foreign Internet service providers will release subscriber information and logged IP addresses to U.S. law enforcement without a formal demand. This reform is necessary to speed the pace at which cyber attacks are traced and investigated.

CONCLUSION

Each day, online newsletters and trade journals report newly discovered computer security vulnerabilities.[76] Most of the hackers who exploit these vulnerabilities lack the political motivation and malicious intent of terrorists or hostile nations. For this reason, most refrain from inflicting the maximum possible damage on compromised systems, and they rarely, if ever, seek to maim or kill. Because so many hackers are content merely to deface the systems they compromise, people may underestimate the havoc true cyber terrorists or hostile nations engaged in "information warfare" could wreak on the United States. In particular, the effects of a compound attack—integrating physical and cyber attacks—could be devastating.

Although cyber terrorists and nation-states may be more malicious and destructive than other hackers, all rely on the same methods and vulnerabilities to penetrate computer systems. As a result, the best defense against cyberterrorism is to improve mainstream computer security. Government must expand institutions that respond to security breaches; expand both formal and informal mechanisms for international cooperation in the investigation and extradition of cyber attackers; and invest in basic research that identifies "the fundamental principles that underlie complex, interconnected infrastructures."[77] However, patching existing systems is an essential but temporary solution; the next generation of information technologies must build improved security

[76] For a daily compilation of cybersecurity news stories, see "Security in the News" at <news.ists.dartmouth.edu/todaysnews.html>.

[77] OSTP, *White Paper on the Institute for Information Infrastructure Protection.*

into their basic structures. This requires an unprecedented level of cooperation between public and private entities.

EXECUTIVE SESSION ON DOMESTIC PREPAREDNESS

JOHN F. KENNEDY SCHOOL OF GOVERNMENT
HARVARD UNIVERSITY

The John F. Kennedy School of Government and the U.S. Department of Justice have created the Executive Session on Domestic Preparedness to focus on understanding and improving U.S. preparedness for domestic terrorism. The Executive Session is a joint project of the Kennedy School's Belfer Center for Science and International Affairs and Taubman Center for State and Local Government.

The Executive Session convenes a multi-disciplinary task force of leading practitioners from state and local agencies, senior officials from federal agencies, and academic specialists from Harvard University. The members bring to the Executive Session extensive policy expertise and operational experience in a wide range of fields - emergency management, law enforcement, national security, law, fire protection, the National Guard, public health, emergency medicine, and elected office - that play important roles in an effective domestic preparedness program. The project combines faculty research, analysis of current policy issues, field investigations, and case studies of past terrorist incidents and analogous emergency situations. The Executive Session is expected to meet six times over its three-year term.

Through its research, publications, and the professional activities of its members, the Executive Session intends to become a major resource for federal, state, and local government officials, congressional committees, and others interested in preparation for a coordinated response to acts of domestic terrorism.

***For more information on the Executive Session on Domestic Preparedness, please contact*:**

Rebecca Storo, Project Coordinator, Executive Session on Domestic Preparedness
John F. Kennedy School of Government, Harvard University
79 John F. Kennedy Street, Cambridge, MA 02138
Phone: (617) 495-1410, Fax: (617) 496-7024
Email: esdp@ksg.harvard.edu
http://www.esdp.org

BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS

JOHN F. KENNEDY SCHOOL OF GOVERNMENT
HARVARD UNIVERSITY

BCSIA is a vibrant and productive research community at Harvard's John F. Kennedy School of Government. Emphasizing the role of science and technology in the analysis of international affairs and in the shaping of foreign policy, it is the axis of work on international relations at Harvard University's John F. Kennedy School of Government. BCSIA has three fundamental issues: to anticipate emerging international problems, to identify practical solutions, and to galvanize policy-makers into action. These goals animate the work of all the Center's major programs.

The Center's Director is Graham Allison, former Dean of the Kennedy School. Stephen Nicoloro is Director of Finance and Operations.

BCSIA's *International Security Program (ISP)* is the home of the Center's core concern with security issues. It is directed by Steven E. Miller, who is also Editor-in-Chief of the journal, *International Security*.

The *Strengthening Democratic Institutions (SDI)* project works to catalyze international support for political and economic transformation in the former Soviet Union. SDI's Director is Graham Allison.

The *Science, Technology, and Public Policy (STPP)* program emphasizes public policy issues in which understanding of science, technology and systems of innovation is crucial. John Holdren, the STPP Director, is an expert in plasma physics, fusion energy technology, energy and resource options, global environmental problems, impacts of population growth, and international security and arms control.

The *Environment and Natural Resources Program (ENRP)* is the locus of interdisciplinary research on environmental policy issues. It is directed by Henry Lee, expert in energy and environment. Robert Stavins, expert in economics and environmental and resource policy issues, serves as ENRP's faculty chair.

The heart of the Center is its resident research staff: scholars and public policy practitioners, Kennedy School faculty members, and a multi-national and inter-disciplinary group of some two dozen pre-doctoral and post-doctoral research fellows. Their work is enriched by frequent seminars, workshops, conferences, speeches by international leaders and experts, and discussions with their colleagues from other Boston-area universities and research institutions and the Center's Harvard faculty affiliates. Alumni include many past and current government policy-makers.

The Center has an active publication program including the quarterly journal *International Security*, book and monograph series, and Discussion Papers. Members of the research staff also contribute frequently to other leading publications, advise the government, participate in special commissions, brief journalists, and share research results with both specialists and the public in a wide variety of ways.

BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS

RECENT DISCUSSION PAPERS

For a complete lising of BCSIA Publications, please visit www.ksg.harvard.edu/bcsia

---

2002-08 Plantinga, Andrew J., Ruben Lubowski, and Robert N. Stavins. "The Effects of Potential Land Development on Agricultural Land Prices."

2002-07 Mayer-Schonberger, Viktor. "Emergency Communications: The Quest for Interoperability in the United States and Europe."

2002-06 Beering, Peter S., Paul Maniscalco, Hank Christen, Steve Storment, and A.D. Vickery. "Winning Plays: Essential Guidance from the Terrorism Line of Scrimmage."

2002-05 Siebenhuner, Bernd. "How Do Scientific Assessments Learn? A Comparative Study of the IPCC and LRTAP."

2002-04 Pangi, Robyn. "Consequence Management in the 1995 Sarin Attacks on the Japanese Subway System."

2002-03 Sauer, Tom. "Beyond the ABM Treaty: A Plea for a Limited NMD System."

2002-02 Orenstein, Mitchell and Martine Haas. "Globalization and the Development of Welfare States in Post-communist Europe."

2002-01 Lahsen, Myanna. "Brazilian Climate Epistemers' Multiple Epistemes: Shared Meaning, Diverse Identities, and Geopolitics in Global Change Science."

2001-22 de Bruijn, Theo and Vicki Norberg-Bohm. "Voluntary, Collaborative, and Information-Based Policies: Lessons and Next Steps for Environmental and Energy Policy in the United States and Europe."

2001-21 Gallager, Kelly Sims. "U.S.-China Energy Cooperation: A Review of Join Activities Related to Chinese Energy Development Since 1980."

2001-20 Zhao, Jimin. "Reform of China's Energy Institutions and Policies: Historical Evolution and Current Challenges."

2001-19 Alcock, Frank. "Embeddedness and Influence: A Contrast of Assessment Failure in New England and Newfoundland."

2001-18 Stavins, Robert. "Lessons from the American Experiment with Market-Based Environmental Policies."

2001-17 Research and Assessment Systems for Sustainability Program. "Vulnerability and Resilience for Coupled Human-Environment Systems: Report of the Research and Assessment Systems for Sustainability Program 2001 Summer Study."

2001-16 Eckley, Noelle. "Designing Effective Assessments: The Role of Participation, Science and Governance, and Focus."

2001-15 Barbera, Joseph A., Anthony Macintyre, and Craig DeAtley. "Ambulances to Nowhere: America's Critical Shortfall in Medical Preparedness for Catastrophic Terrorism."

2001-14 Cavanagh, Sheila. "Thirsty Colonias" Determinants of Water Service Coverage in South Texas."

2001-13 Rapporteur's Rapport. "Workshop on the Role of Science and Economics in Setting Environmental Standards."

2001-12 Hogan, William. "Electricity Market Restructuring: Reforms of Reforms."

2001-11 Koblentz, Gregory. "A Survey of Biological Terrorism and America's Domestic Preparedness Program."

2001-10 Lee, Henry, Philip Vorobyov, and Christine Breznik. "Entering Russia's Power Sector: Challenges in Creating a Credible Carbon Trading System."

2001-09 Pate, Jason and Gavin Cameron. "Covert Biological Weapons Attacks Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture."

2001-08 Carment, David. "The Role of Bias in Third Party Intervention: Theory and Evidence."

2001-07 Foster, Charles, H. W., and James N. Levitt. "Reawakening in the Beginner's Mind: Innovations in Environmental Practice."

2001-06 Donohue, Laura. "In the Name of National Security: U.S. Counterrorism Measures, 1960-2000."

2001-05 Koblentz, Gregory. "Overview of Federal Programs to Enhance State and Local Preparedness for Terrorism with Weapons of Mass Destruction."

2001-04 Kayyem, Juliette. "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning."

2001-03 Foster, Charles H.W. and James S. Hoyle. "Preserving the Trust: The Founding of the Massachusetts Environmental Trust."

2001-2 Coglianese, Cary. "Is Consensus an Appropriate Basis for Regulatory Policy?"

2001-1 Donohue, Laura K. and Juliette N. Kayyem. "The Rise of the Counterterrorist States."

TAUBMAN CENTER FOR STATE AND LOCAL GOVERNMENT

JOHN F. KENNEDY SCHOOL OF GOVERNMENT
HARVARD UNIVERSITY

The Taubman Center for State and Local Government focuses on public policy and management in the U.S. federal system. Through research, participation in the Kennedy School's graduate training and executive education programs, sponsorship of conferences and workshops, and interaction with policy makers and public managers, the Center's affiliated faculty and researchers contribute to public deliberations about key domestic policy issues and the process of governance. While the Center has a particular concern with state and local institutions, it is broadly interested in domestic policy and intergovernmental relations, including the role of the federal government.

The Center's research program deals with a range of specific policy areas, including urban development and land use, transportation, environmental protection, education, labor- management relations and public finance. The Center is also concerned with issues of governance, political and institutional leadership, innovation, and applications of information and telecommunications technology to public management problems. The Center has also established an initiative to assist all levels of government in preparing for the threat of domestic terrorism.

The Center makes its research and curriculum materials widely available through various publications, including books, research monographs, working papers, and case studies. In addition, the Taubman Center sponsors several special programs:

The Program on Innovations in American Government, a joint undertaking by the Ford Foundation and Harvard University, seeks to identify creative approaches to difficult public problems. In an annual national competition, the Innovations program awards grants of $100,000 to 15 innovative federal, state, and local government programs selected from among more than 1,500 applicants. The program also conducts research and develops teaching case studies on the process of innovation.

The Program on Education Policy and Governance, a joint initiative of the Taubman Center and Harvard's Center for American Political Studies, brings together experts on elementary and secondary education with specialists in governance and public management to examine strategies of educational reform and evaluate important educational experiments.

The Saguaro Seminar for Civic Engagement in America is dedicated to building new civil institutions and restoring our stock of civic capital.

The Program on Strategic Computing and Telecommunications in the Public Sector carries out research and organizes conferences on how information technology can be applied to government problems -- not merely to enhance efficiency in routine tasks but to produce more basic organizational changes and improve the nature and quality of services to citizens.

The Executive Session on Domestic Preparedness brings together senior government officials and academic experts to examine how federal, state, and local agencies can best prepare for terrorist attacks within U.S. borders.

The Program on Labor-Management Relations links union leaders, senior managers and faculty specialists in identifying promising new approaches to labor management.

The Internet and Conservation Project, an initiative of the Taubman Center with additional support from the Kennedy School's Environment and Natural Resources Program, is a research and education initiative. The Project focuses on the constructive and disruptive impacts of new networks on the landscape and biodiversity, as well as on the conservation community.

TAUBMAN CENTER FOR STATE AND LOCAL GOVERNMENT

RECENT DISCUSSION PAPERS

A complete publications list is available at www.ksg.harvard.edu/taubmancenter/

2002 Peterson, Paul. "While America Slept," $6.

2001 Borins, Sandford. "The Challenge of Innovating in Government," $5.

2001 Donohue, Laura K. "In the Name of National Security: U.S. Couterterrorist Measures, 1960-2000."

2001 Donohue, Laura K. and Juliette N. Kayyem. "The Rise of the Counterrorist States."

2001 Executive Session on Domestic Preparedness. "A New National Priority: Enhancing Public Safety and Health Through Domestic Preparedness."

2001 Gomez-Ibanez, Jose A. "Deregulating Infrastructure: Breaking Up Is Hard to Do," $6.

2001 Greene, Jay P. "An Evaluation of the Florida A-Plus Accountability and School Choice Program," $6.

2001 Harvard Policy Group on Network-Enabled Services and Government. "Use for IT Strategic Innovation, Not Simply Tactical Automation," $7.

2001 Harvard Policy Group on Network-Enabled Services and Government. "Utilize Best Practices in Implementing IT Initiatives," $7.

2001 Kayyem, Juliette N. "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning."

2001 Koblentz, Gregory D. "Overview of Federal Programs to Enhance State and Local Preparedness for Terrorism with Weapons of Mass Destruciton."

2001 Levitt, James N. and Charles H. W. Foster. "Reawakening the Beginner's Mind: Innovation in Environmental Practice."

2001 Pate, Jason and Gavin Cameron. "Covert Biological Weapons Attacks Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture."

2001 Peterson, Paul, David Campbell and Martin West. "An Evaluation of the Basic Fund Scholarship Program in the San Francisco Bay Area, California," $6.

2000 Donohue, Laura. "Civil Liberties, Terrorism, and Liberal Democracy: Lessons from the United Kingdom."

2000 Falkenrath, Richard A. "Analytic Models and Policy Prescription: Understanding Recent Innovation in U.S. Counterterrorism."

2000 Falkenrath, Richard A. "The Problems of Preparedness: Challenges Facing the U.S. Domestic Preparedness Program."

2000 Fung, Archon, Charles Sabel and Dara O'Rourke. "Ratcheting Labour Standards: How Open Competition Can Save Ethical Sourcing," $6.