CHAPTER 1

Cyber Crime and Security

The Transnational Dimension

Abraham D. Sofaer

Seymour E. Goodman

The information infrastructure is increasingly under attack by cyber criminals. The number, cost, and sophistication of attacks are increasing at alarming rates. They threaten the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information. Some forms of attack also pose a growing threat to the public, and to critical infrastructures.

Much has been said about the threat posed by cyber crime, including terrorism, but little has been done to protect against what has become the most costly form of such crime: transnational attacks on computers and the information infrastructure. Measures thus far adopted by the private and public sectors fail to provide an adequate level of security against these attacks. The Internet and other aspects of the information infrastructure are inherently transnational. A transnational response sufficient to meet these transnational challenges is an immediate and compelling necessity.

The challenge of controlling transnational cyber crime requires a full range of responses, including both voluntary and legally mandated cooperation. Both the private and public sectors are now actively pursuing transnational initiatives, ranging in form from voluntary, informal exchange of information to a multilateral treaty proposed by the Council of Europe (COE) to establish common crimes and a substantial degree of cooperation in the investigation and prosecution of such crimes.

Public declarations and voluntary international cooperation have no doubt helped in dealing with transnational attacks. Funds are being made available to enhance the technological capacities of national law enforcement personnel engaged in cyber investigations, and through international cooperation, some attacks have been traced, and some perpetrators have been punished. But public pronouncements, educational programs, and voluntary cooperation are not enough. The sources of many transnational attacks have never been determined, and perpetrators of many of the most damaging attacks, even when identified, go unpunished. A great disparity exists, moreover, in the legal and technological capacity of states to meet the challenges of preventing, investigating, and prosecuting cyber crime.

An effective program against transnational cyber crime will require legal cooperation among states that involves the enforcement of agreed standards of conduct. A reasonably broad consensus exists among states concerning many forms of conduct that should be treated as cyber crime within national borders. This consensus must be translated into a legal regime in which all states that are connected to the Internet prohibit forms of conduct widely regarded as destructive or improper. In addition, much remains to be done to encourage and, as soon as practicable, to require states to adopt common positions to facilitate cooperation in investigation, the preservation of evidence, and extradition. States must establish and designate cross-patent agencies to deal with transnational issues, and to cooperate with counterparts throughout the world. To develop and secure the universal adoption of technological and policy standards to defend against, prosecute, and deter cyber crime and terrorism, states should create an international agency, along the lines of the International Civil Aviation Organization (ICAO) but designed to reflect the particular needs and nature of the cyber world. International cooperation must include an effective program to upgrade the capacities of states that lack the technological resources to cooperate in a comprehensive international regime. These measures, though far-reaching by comparison with current policies, can be fashioned to maximize private-sector participation and control, to ensure that privacy and other human rights are not adversely affected and so as not to impinge on the national security activities and interests of States Parties.

I. Scope of the Problem

A summary of the problem of cyber crime and terrorism was presented at the Stanford Conference by Peter G. Neumann, principal scientist at the Computer Science Laboratory, SRI International. He stated:

> We are becoming massively interconnected. Whether we like it or not, we must coexist with people and systems of unknown and unidentifiable trustworthiness (including unidentifiable hostile parties), within the U.S. and elsewhere. Our problems have become international as well as national, and cannot be solved only locally.
>
> Computer-related systems tend to fall apart on their own, even in the absence of intentional misuse. However, misuse by outsiders and insiders and the presence of malicious code . . . present some enormously difficult challenges that are not being adequately addressed at present. . . .
>
> Computers and communications are increasingly being used in almost every imaginable application. However, our computer-communication systems are not dependably secure, reliable, or robust. Reliability, fault tolerance, security, and overall system survivability

> are all closely interrelated. There are fundamental vulnerabilities in the existing information system infrastructures, and serious risks that those vulnerabilities will be exploited—with possibly very severe effects.
>
> Our national infrastructures depend not only on our interconnected information systems and networks, but also on the public switched network, the air-traffic control systems, the power grids, and many associated control systems—which themselves depend heavily on computers and communications.
>
> Global problems can result from seemingly isolated events, as exhibited by the early power-grid collapses, the 1980 ARPANET collapse, and the 1990 long-distance collapse—all of which began with single-point failures.
>
> Our defenses against a variety of adversities—from intentional misuse to hardware flaws and software bugs to environmental disturbances—are fundamentally inadequate.
>
> Our defenses against large-scale coordinated attacks are even more inadequate. . . .
>
> The risks of cyber terrorism and cyber crime vastly outweigh our abilities to control those risks by technological means, although technology can help and should be vigorously pursued. There are many important problems, such as providing better defenses against denial of service attacks, outsiders, and insiders. Socio-politico-economic measures must also be considered.[1]

2. Costs of Cyber Crime

The costs of cyber crime are difficult to measure, but by any reasonable standard they are substantial and growing exponentially. The most comprehensive available source of data on costs is compiled annually by the Computer Security Institute (CSI), with the participation of the

[1] Peter G. Neumann, "Information System Adversities and Risks," presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California, December 6–7, 1999, pp. 1–2, 3. As of early 2000, some 210 countries were connected to the Internet, which had about 300 million users; the number of users is expected to rise to one billion by 2005. See Martin Stone, *Newsbytes*, March 22, 2000, which was available at ⟨*http://www.newsbytes.com*⟩.

FBI's Computer Intrusion Squad. The CSI survey for 2000, edited by Stanford Conference participant Richard Power, is based on 643 responses from computer security practitioners in U.S. corporations and government agencies.[2] It establishes that computer security breaches are widespread, diverse, and costly. Respondents are investing heavily in a variety of security technologies, at a cost estimated by the International Data Corporation to grow from $2 billion in 1999 to $7.4 billion in 2003.[3] These investments are dramatic evidence of the huge costs being inflicted by cyber crime. To these amounts must be added the costs of cyber crime insurance, a new coverage for an expanding market.[4]

In spite of the costly defensive measures thus far adopted, CSI/FBI survey respondents experiencing unauthorized use of their computer systems increased from 42 percent in 1996 to 70 percent in 2000; those not experiencing such events declined from 37 percent to 18 percent in the same period. Only 37 percent of all attacks reported in 1996 involved Internet connections; in 2000 this proportion increased to 59 percent, with a corresponding decline in insider attacks. So far, the most serious category of reported financial loss has been through "theft of proprietary information," which appears to include attacks that result in the theft of financial data.[5] Other categories of substantial losses include fraud, virus attacks, denial of service, and sabotage.

Estimating the monetary damage inflicted by cyber crime is diffi-

[2] See Richard Power, ed., "2000 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends* 6 (Spring 2000). See also Richard Power, *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace* (New York: Que/Macmillan Publishing, 2000).

[3] Power, ed., "2000 CSI/FBI Computer Crime and Security Survey," p. 3.

[4] See Carolyn Batt, "Marsh Offers Policy Against Computer Viruses and Fraud," *The Age*, May 31, 2000: "Such insurance does not come cheap. . . . [P]remiums in the United States . . . ranged from $US15,000 to $US700,000," available at 2000 Westlaw (WL) 21651659. See also "On Message," *The Guardian* (London), June 8, 2000: "A survey conducted by Lloyd's showed 75% of firms have no e-commerce insurance cover against damage caused by computer hackers and viruses"; available at 2000 WL 22777128.

[5] See Power, ed., "2000 CSI/FBI Computer Crime and Security Survey," p. 6.

cult but worth attempting, and particularly valuable for tracking relative costs from year to year. The CSI/FBI surveys for the last four years report total losses of about $100,000,000 in 1997, increasing to some $266,000,000 in 2000.[6] Stephen J. Lukasik has found a pattern reflecting a trend in which costs have essentially doubled each year.[7] This progression has been shattered by costs associated with the "I Love You" virus of May 2000, estimated at between $1 and $10 billion. Although the costs reported by respondents include lost time, and may be exaggerated, the reluctance of companies to acknowledge losses tends to result in underreporting.[8] The overall numbers are useful indicators when these uncertainties are taken into account.

3. Transnational Nature of Cyber Crime

At a purely technical level, all messages on the Internet are broken down into "packets" that separate and travel through available routers and servers located throughout the world.[9] Cyber crime goes beyond this technical, transnational dimension and involves senders who deliberately fashion their attacks and other crimes to exploit the potential weaknesses present in the infrastructure's transnational nature. These weaknesses include: (1) a worldwide target pool of computers and users to victimize, or to exploit in denial-of-service or other attacks, which enables attackers to do more damage with no more effort than would be necessary in attacking computers or users in a single state; and (2) the widespread disparities among states, in the legal, regulatory, or policy environment concerning cyber crime, and the lack of a

[6] Ibid., p. 9. See also Richard Power, "Estimating the Cost of Cyber Crime," presentation at the Stanford Conference, December 6–7, 1999, pp. 6–11.

[7] See Stephen J. Lukasik, "Current and Future Technical Capabilities," Chap. 4 in the present volume.

[8] The "FBI estimates that only 17 percent of computer crimes are reported to government authorities." Robert L. Ullman and David L. Ferrera, "Crime on the Internet," *Boston Bar Journal*, Nov./Dec. 1998, n 6.

[9] See Robert E. Kahn and Stephen J. Lukasik, "Fighting Cyber Crime and Terrorism: The Role of Technology," presentation at the Stanford Conference, December 6–7, 1999, pp. 6–11.

sufficiently high degree of international cooperation in prosecuting and deterring such crime.

The most damaging cyber attacks thus far experienced have been transnational, originating in many different countries and aimed at computers everywhere. Here are some prominent examples:[10]

- The so-called "Phonemasters," a "loosely-knit," "12-member" international "hacking ring" headed by Jonathan Bosanac of Rancho Santa Fe, California (near San Diego), who, using the on-line name "The Gatsby," developed a method for gaining access to telephone networks (such as MCI, WorldCom, Sprint, and AT&T), credit-reporting databases (such as Equifax), and even the FBI's own National Crime Information Center, which they utilized in a number of countries.[11] "The breadth of their monkey-wrenching was staggering; at various times they could eavesdrop on phone calls, compromise secure databases, and redirect communications at will. They had access to portions of the national power grid, air-traffic–control systems and had hacked their way into a digital cache of unpublished telephone numbers at the White House. . . . [T]hey often worked in stealth, and avoided bragging about their exploits. . . . Their customers included . . . the Sicilian Mafia. According to FBI estimates, the gang accounted for about $1.85 million in business losses."[12]
- David L. Smith, a New Jersey programmer, pleaded guilty in December 1999 of creating the "Melissa" computer virus and

[10] For more examples, see Power, ed., "2000 CSI/FBI Computer Crime and Security Survey," pp. 6–7; Richard Power, *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare*, 3d ed. (San Francisco: Computer Security Institute, 1999), pp. 1–38.

[11] See Kathryn Balint, "Notorious Hacker, 'The Gatsby,' Gets 18 Months' Prison," *San Diego Union-Tribune*, March 4, 2000, available at 2000 WL 13951675.

[12] See John Simons, "Phone Hex: How a Cyber Sleuth, Using a 'Data Tap,' Busted a Hacker Ring—Audacious 'Phonemasters' Stole Numbers, Pulled Scams, Tweaked Police—A Sex-Line Prank on the FBI," *Wall Street Journal*, October 1, 1999, p. A1, available at 1999 WL-WSJ 24916121.

using an x-rated website to spread it through cyber space via e-mail in March 1999, where it "rampaged personal, government, and corporate computers around the world," "caused worldwide devastation," and was estimated to have done $80 million (or more) in damages.[13]

- From December 1999 through April 2000, five hackers in Moscow stole more than 5,400 credit card numbers belonging to Russians and foreigners from Internet retailers, pocketing more than $630,000 until arrested.[14] The incident pointed up the threat that "Eastern European fraudsters continue to pose . . . for all card issuers, even those with no direct business in the region.[15]
- In 1995–96, from his home in Buenos Aires, a twenty-one-year-old Argentine student, Julio Cesar Ardita, "slipped through the security of . . . systems at Harvard University's

[13] See: "Melissa Virus Exposes Computer Users' Vulnerability," *Japan Computer Industry Scan*, April 12, 1999, available at 1999 WL 9642279; "Battling the Cyberspace Superbugs: With 18,000 Viruses Infecting the World's Computer Networks, the Hunt Is on for the Cyber-Criminals Who Put Them There," *Western Daily Press*, May 5, 2000, available at 2000 WL 3236905; "Melissa Virus Creator Pleads Guilty: A Computer Programmer Admitted on Thursday that He Created and Distributed the Melissa Virus," *Newswire*, December 10, 1999: "In the Federal plea, both sides agreed that the damage amounted to more than $80 million"; available at 1999 WL 6824880.

[14] See "Suspected Russia Hackers Held," *New York Times on the Web/Breaking News from Associated Press*, April 28, 2000, reported at ⟨*http://www.nytimes.com/aponline/i/AP-Russia-Hackers.html*⟩. See also "Hacker Reveals Credit Card Data," ibid., January 10, 2000: a hacker, "a self-described 19-year-old Russian using the name Maxim, sent an e-mail" to the *New York Times* "boasting that he exploited a security flaw in the software used to protect financial information" at the website of an Internet music retailer, CD Universe, and posted credit card numbers he stole from the site "after the retailer refused to pay a $100,000 ransom"; reported at ⟨*http://www.nytimes.com/aponline/a/AP-Credit-Card-Crook.html*⟩.

[15] See Jason Fargo, "Card Fraud's New Hotbed?," 13 *Credit Card Management*, April 1, 2000, p. 9698, available at 2000 WL 10684223; reportedly "shoddy practices" at Union Card Processing Company, a Moscow-based firm that processes automated teller machine transactions for Russian banks, "allowed criminals to obtain card data with which they then manufactured counterfeit cards."

Faculty of Arts and Science, the U.S. Defense Department, the U.S. Naval Command, the San Diego-based Control and Ocean Surveillance Center, the Washington-based Naval Research Lab, NASA's Ames Research Center and Jet Propulsion Laboratory, and the Los Alamos National Laboratory in New Mexico."[16] His actions were not criminal in Argentina, and his extradition to the U.S. was refused, although he later surrendered voluntarily.

- Reports of persistent, international attacks on official government websites throughout the world in 1999–2000 appeared with great frequency. Some of the notable ones include: (1) Hackers breaking into the website of the Ministry of Finance of Romania in November 1999 to introduce bogus taxes and to change the official exchange rate of the national currency.[17] (2) Recurrent Taiwan-China "hacker" wars in 1999 and 2000 in which attackers broke into various government and business websites, penetrating protective firewall software with seeming ease.[18] (3) Frequent transnational attacks on sensitive military and other national security networks of many governments, as well as public service websites/infrastructure at the national and local levels.[19]

[16] See David Berlind, "Reno's Border Patrol Made Ineffective," *PC Week*, April 8, 1996, p. 78.

[17] See "Hackers Alter Romanian Money Rate," *New York Times on the Web/ Breaking News from Associated Press*, November 3, 1999, reported at ⟨*http:// www.nytimes.com/aponline/i/AP-Romania-Hackers.html*⟩.

[18] See "Taiwan-China Hackers' War Erupts," *New York Times on the Web/ Breaking News from Associated Press*, August 9, 1999, reported at ⟨*http:// www.nytimes.com/aponline/i/AP-Taiwan-China-Hackers.html*⟩; "Taiwan Spy Agency Website Hacked," ibid., March 6, 2000, reported at ⟨*http://www.nytimes.com/ aponline/i/AP-Taiwan-China-Hackers.html*⟩.

[19] See, e.g., Stephen J. Glain, "Blind Arab Brothers, Allegedly Hackers, Disconcert Israel: They're on Trial for Tapping into Defense Phone System to Commit 'Cybercrimes,'" *Wall Street Journal*, October 21, 1999, p. A1; Daniel Verton, "Cyberattacks Against DOD up 300 Percent This Year," reported at *CNN.com*, November 5, 1999; "Swedes Charged with U.S. Hacking," *New York Times on the Web/ Breaking News from Associated Press*, August 16, 1999, reported at ⟨*http://*

- The "I Love You" virus was propagated from the Philippines in May 2000.[20] Estimates of the damage it caused range up to $10 billion, mostly in lost work time. U.S. investigators pressed to have the suspects in the attack—computer programming students from the Philippines—arrested and prosecuted, and Filipino investigators attempted to do so under a 1998 law prohibiting the use of "access devices," such as credit cards, to defraud. The Chief State Counsel concluded, however, that this law could not be used, since "the intention of a computer hacker . . . is not to defraud but to destroy files."[21] The Philippines adopted a law punishing those who spread computer viruses with up to three years' imprisonment and fines from $2,350 to a maximum "commensurate" with the damage caused.[22] The new law will not apply retroactively, however, so this costly act has gone unpunished.[23]

www.nytimes.com/aponline/i/AP-Sweden-Hackers.html〉; "Hacker Takes Over Hawaii's Website," ibid., July 6, 1999: "We've had to block out the entire country of Brazil because we've had so many crack attempts from so many locations in Brazil"; reported at 〈*http://www.nytimes.com/aponline/a/AP-Computer-Hacker.html*〉.

[20] See "Report on Love Bug Virus Submitted," *New York Times on the Web/Breaking News from Associated Press*, June 13, 2000, reported at 〈*http://www.nytimes.com/aponline/i/AP-Philippines-Love-Bug.html*〉. Note that the 2000 CSI/FBI report predates the extreme disruption and costs associated with the rapid spread of the "I Love You" computer virus around the world from the Philippines in May 2000.

[21] See "Philippines Seek 'Love Bug' Law," *New York Times on the Web/Breaking News from Associated Press*, May 17, 2000 (remarks of Elmer Bautista), reported at 〈*http://www.nytimes.com/aponline/i/AP-Computer-Love-Bug.html*〉.

[22] See "Philippines Addresses Web Crimes," *New York Times on the Web/Breaking News from Associated Press*, June 14, 2000, reported at 〈*http://www.nytimes.com/aponline/i/AP-Philippines-Love-Bug.html*〉.

[23] "A lack of applicable laws forced prosecutors to dismiss all charges yesterday against the man accused of releasing the 'Love Bug,' a computer virus that caused billions of dollars in damages worldwide." See "'Love Bug' Suspect Set Free," *Palo Alto Daily News*, August 22, 2000, p. 9; Robert Frank, "'Love Bug' Case Against Student Gets Dismissed As Laws Lag," *Wall Street Journal*, August 22, 2000, p. A20.

4. Weaknesses of the Current System

The open and defiant manner in which hackers currently operate reflects the weakness of the legal, defensive, and investigative capacities of the current system.[24] They plan and discuss proposed forms of attack on websites, exchanging ideas and comments.[25] These activities enabled Thomas A. Longstaff of the Computer Emergency Response Team (CERT)/Coordination Center (CC), Software Engineering Institute (SEI) at Carnegie Mellon University to predict at the Stanford Conference that a new and very harmful, distributed form of denial-of-service attack was the next likely threat. He described precisely the method that was used by hackers in the subsequent worldwide February 2000 attacks—on CNN, eBay, Amazon.com, and others—to plant programs in computers around the globe that enabled hackers to send so many messages to particular IP addresses that they were rendered inoperable. Though law enforcement personnel were able to

[24] Hackers adopt nicknames reflecting their intentions and attitudes, such as "Badman," "Masters of Deception," "Legion of Doom," and "Mafiaboy." See "Teen Hacker Appears in Court," *Yahoo! News/Associate Press*, June 6, 2000 (story relating to a 15-year-old Canadian nicknamed "Mafiaboy," who is alleged to have instigated a February 8, 2000, cyber attack on the CNN website, one of a series of attacks that targeted major sites including Yahoo!, eBay, and Amazon.com), at ⟨*http://dailynews.yahoo.com/h/ap/20000606/wl/canada_teen_hacker_1.html*⟩.

[25] Numerous "hacker" and/or cyber security/cyber attack-related websites exist, with many, varying objectives. Compare, e.g., ⟨*http://www.attrition.org/*⟩ ("a computer security website dedicated to the collection, dissemination, and distribution of information about the industry for anyone interested in the subject") with ⟨*http://phrack.infonexus.com/*⟩ (classified by Yahoo.com as "technical info. for hackers") and ⟨*http://www.hackernews.com/*⟩ ("Our first mission is to deliver the real news from the computer underground *for* the computer underground"). See also, "Crowds Awaited at Hacker Convention," *New York Times on the Web/Breaking News from Associated Press*, July 8, 1999 (story about the 1999 "DefCon," an annual hackers convention in Las Vegas begun with only 100 attendees in 1993, which as of the July 1999 meeting was attracting thousands), reported at ⟨*http://www.nytimes.com/aponline/f/AP-Hackers-Convention.html*⟩. Also: ⟨*http://www.defcon.org/*⟩ (website for the 2000 "DefCon 8.0").

anticipate this type of attack, they were not able to prevent it, and security personnel at CNN, Yahoo!, Amazon.com, and others could not defend against it. After several months of investigation, in April 2000, the Royal Canadian Mounted Police (RCMP) arrested a Montreal teenager on suspicion of having caused the CNN and other shutdowns, but the extent to which the culprit (or culprits) may be successfully prosecuted is in doubt, and deterrence of those not caught and punished, as well as of other would-be attackers, seems unlikely.[26] These troubling failures stem from serious weaknesses in the authority and capacities of states to protect cyber systems from attacks.[27]

Escalating Dangers of Attacks

New forms of denial-of-service and other destructive types of attack, such as the "I Love You" virus, have been openly discussed, or uncovered, and cyber copycats continue to be active, replicating or modifying attacks into yet more dangerous forms—such as the "Killer Resume" follow-on to "I Love You"—with virtually complete impunity.

Knowledgeable individuals have anticipated new forms of cyber attack that may be even more costly than prior ones. For example, a virus similar to "I Love You," called "Timofonica" (Spanish for "phone prank"), that has been intercepted in Europe is designed to attack cell phones, and can easily be altered to attack pagers and other hand-held devices such as Palm Pilots and Microsoft Pocket PC com-

[26] See "Teen Hacker Appears in Court," *Yahoo! News/Associate Press*, June 6, 2000; "Hacker 'Mafiaboy' Likely to Face More Charges," *Yahoo! News/Reuters*, June 7, 2000 (the suspect could face "up to two years in a youth detention center and a . . . $675 fine, if found guilty"), available at ⟨*http://dailynews.yahoo.com/h/nm/20000607/wr/mafiaboy_dc_1.html*⟩; "Canadian Hacker Pleads Not Guilty," *New York Times on the Web/Breaking News from Associated Press*, August 3, 2000, reported at ⟨*http://www.nytimes.com/aponline/i/AP-Canada-Teen-Hacker.html*⟩.

[27] See generally the excellent report prepared by McConnell International, "Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information" (December 2000), available at ⟨*http://www.mcconnellinternational.com*⟩.

puters.[28] Vincent Gullatto, director of the AVERT antivirus lab at the San Jose, California–based Network Associates, which makes McAfee antivirus software, has noted that, once hand-held devices become sophisticated enough to use "miniature automation programs known as macros, the potential to wreak havoc will grow."[29] Similarly, as reliance on wireless transmission increases, the danger posed by forms of jamming will grow. An even more threatening development is predicted by Israeli computer security expert Ofer Elzam. In addition to "an increasing number of viruses, worms, and vandals" he expects will populate the cyber world, he anticipates "something far more lethal and threatening—the Trojan horse."[30] These devices, Elzam states, "are smart spying machines or engines that can sit in a PC for years and give anyone access to the most personal information stored on the computer," without creating any sign of damage: "Things are going to get much, much worse in every field of Internet security," in part because "the more complicated things get the more holes there are."[31] It was reported on June 18, 2000, that an undisclosed number

[28] See "New Virus Targets Handheld Devices," *New York Times on the Web/ Breaking News from Associated Press*, June 6, 2000, reported at ⟨*http:// www.nytimes.com/aponline/f/AP-Cell-Phone-Virus.html*⟩

[29] Ibid.

[30] See Nicky Blackburn and Meir Ronne, "Forget Viruses, the Trojans Are Coming," *Jerusalem Post*, May 28, 2000, p. 8, available at 2000 WL 8258478. "Like its Greek namesake, Trojan horses are weapons hidden within a friendly exterior. They come as seemingly innocuous e-mails or lurk in websites on the Net. A user may receive an innocent-looking e-mail, but embedded within the attachment, or in some cases even the HTML message itself, is a coded page, which connects your PC to a website. From there a small Trojan horse, often as little as 6k, is downloaded into your computer and the hacker, blackmailer, competitor, or just good, old-fashioned enemy is alerted, often through ICQ messaging, that the computer has been penetrated. The hacker can then add however many programs he wants to the victim's computer, allowing him access to the most personal files, be they financial plans or letters to a lover. In some circumstances the hacker can even have remote control of the computer itself, a threat with many worrying implications. The same can happen to a user while surfing the Internet. A user might be lured to a particular site by promises of a free holiday or entry into a sweepstakes and while . . . visiting a Trojan horse or a virus is downloaded to their computer."

[31] Ibid.

of America Online (AOL) employee accounts had been compromised by a Trojan horse.[32] The trend toward increasingly dangerous attacks is well established.

The danger of cyber attacks extends to matters of intense public concern. Cyber terrorism has not yet resulted in any public disaster, but attacks on the websites and cyber systems of public agencies are common.[33] Favorite targets include defense and intelligence agencies.[34] Although for the most part these attacks are amateurish and are blocked successfully or result in only superficial damage to websites,[35] a significant number have shut down websites, and some have penetrated much further.[36]

[32] See "AOL Confirms Hacking of Employee Accounts," *Chicago Tribune*, June 18, 2000, p. 7, available at 2000 WL 3676402. Other scientists have characterized the most highly connected nodes, through which most messages are channeled, as the Achilles' heel of the Internet. See "Scientists Spot Achilles' Heel of the Internet," *HPCwire*, July 28, 2000, which was distributed through 〈*trial@hpcwire.tgc.com*〉.

[33] See: "Hackers Become an Increasing Threat," *New York Times on the Web/Breaking News from Associated Press*, July 7, 1999, which was reported at 〈*http://www.nytimes.com/aponline/w/AP-Hacker-Threat.html*〉; Verton, "Cyberattacks Against DOD up 300 Percent This Year," *CNN.com*, November 5, 1999.

[34] See, e.g.: "Hackers Attack Army's Internet Site," *New York Times on the Web/Breaking News from Associated Press*, June 28, 1999, reported at 〈*http://www.nytimes.com/aponline/w/AP-Army-Hacked.html*〉; "Taiwan Spy Agency Website Hacked," ibid., March 6, 2000. Hackers have reportedly even disrupted service to the top-secret U.S. Air Force "Area 51" site in Nevada. "Hacker Disrupted Service to Area 51," ibid., April 21, 2000, reported at 〈*http://www.nytimes.com/aponline/a/AP-Area-51-Hacker.html*〉. The FBI has also "acknowledged . . . that electronic vandals" have been able to "shut down its own . . . site for hours." See "FBI Admits Its Site Was Attacked," ibid., February 25, 2000, reported at 〈*http://www.nytimes.com/aponline/w/AP-Hacker-Investigation.html*〉.

[35] See, e.g., "White House Hacker Faces Prison," ibid., November 22, 1999, reporting that the White House website attack consisted primarily of slight alterations to the site including "the phrase, 'following peeps get some shouts'—hacker slang for 'hello,'" reported at 〈*http://www.nytimes.com/aponline/w/AP-White-House-Hacker.html*〉.

[36] Consider the 1998 "Solar Sunrise" attack of "young hackers from California and Israel" who "were able to penetrate numerous Department of Defense computers and gain 'root' access, meaning they had the capability to shut the systems down or steal or alter important information." See "Statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Before the

To classify such attacks as pranks merely because they seem politically aimless is mistaken. Politically aimless conventional attacks on public infrastructure are an established form of terrorism—the hallmark of anarchists. Where such attacks are intended to, and do, cause serious damage, they should, and will, be treated as terrorist acts. Furthermore, when states sponsor such attacks, they take on an additional political dimension; the FBI's National Infrastructure Protection Center (NIPC) appears to believe that state-sponsored acts have already been undertaken.[37] Among the nation's critical infrastructure most vulnerable to cyber attacks are transportation (especially air travel), power, defense, water, and medical care. The Stanford Conference focused on the dangers to civil aviation as exemplifying this danger.[38]

Disparities in National Laws of Protection and Cooperation

A significant weakness in the current system is the disparity among individual states in the laws and practices necessary to permit them to investigate and prosecute cyber crime effectively.[39] Though states may

Senate Committee on Judiciary," *Hearing on Internet Security and Privacy*, May 25, 2000, available at ⟨*http://www.senate.gov/judiciary/52520mav.htm*⟩.

[37] Ibid.: "Over the past several years we have seen a broad spectrum of computer crimes ranging from defacement of websites by juveniles to *sophisticated intrusions that we suspect may be sponsored by foreign powers*, and everything in between" [emphasis added]. See generally the 1998 Center for Strategic and International Studies (CSIS) report, *Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo* (Washington, D.C.: CSIS, 1998), and Georgetown University Professor Dorothy E. Denning's reactions to it, discussed in Paul Talacko, "Computer Hackers and Cyberterrorists: Close Watch Around the Clock," *Financial Times*, October 4, 2000, p. iv.

[38] See the essays in Chap. 3 of this volume. The potential for attacks on the power infrastructure is discussed by Stephen J. Lukasik in "Metrics for Assessing the Vulnerability of the Electric Power Grid to Cyberattack," unpublished ms., Consortium for Research on Information Policy and Security (CRISP), Stanford University, September 11, 1999.

[39] See, e.g., "Cyberattackers Target Latin America," *New York Times on the Web/Breaking News from Associated Press*, February 16, 2000: "Internet vandals are wreaking havoc in Latin America's fast-growing cyberspace frontier" where "it's even

have agreements in place to cooperate against and extradite or prosecute for conventional crimes involving the *use* of computers, no international agreement yet exists on such cooperation for criminal attacks on computers and the information infrastructure.[40] In several highly significant cases, investigations and prosecutions have been stymied by this deficiency. In 1996, Argentine hacker Julio Cesar Ardita escaped relatively unscathed after having compromised numerous sensitive and proprietary computer networks, including some in the U.S. Department of Defense (DOD), from his Buenos Aires home. Argentina refused to extradite Ardita to the U.S., because his intrusion did not constitute an extraditable crime. Another very serious series of attacks on national security sites in the U.S. and Israel—subsequently code-named "Solar Sunrise" by the DOD—was conducted by "a trio of teenage hackers" in February 1998.[41] These individuals were identified and were ultimately prosecuted for their criminal conduct, but not without significant difficulties encountered by U.S. and Israeli investigators owing to the lack of established commitments and pro-

easier to break into many websites because Internet culture is relatively immature and authorities are generally ill-prepared to respond" and governments "have done little to address digital crime," reported at ⟨*http://www.nytimes.com/aponline/i/AP-Latin-America-Hacker-Attacks.html*⟩.

[40] This distinction is part of the three-category breakdown of the role of computers in crime found in *The Electonic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet* (March 2000), Part II.A. Inexplicably, this report focuses "primarily" on the category of using computers as a tool for crime. It recognizes the need for international cooperation but makes no recommendations for dealing with crimes against computers—in spite of the following conclusions (in Part III.E.1 & 2): "When one country's laws criminalize high-tech and computer-related crime and another country's laws do not, cooperation to solve a crime, as well as the possibility of extraditing the criminal to stand trial, may not be possible. . . . Although bilateral cooperation is important in pursuing investigations concerning unlawful conduct involving the use of the Internet, multilateral efforts are a more effective way to develop international policy and cooperation in this area. The reason for this stems from the nature of the Internet itself."

[41] See, e.g., William Jackson, "1999: The Year of Computer Security," *Newsbytes News Network*, December 15, 1998, available at 1998 WL 20720335.

cedures. Boaz Gutman, chief superintendent of Computer Crime Division, National Anti-Fraud Investigation Unit, Israeli National Police, detailed some of the difficulties at the Stanford Conference. He noted that, though voluntary cooperation is better than none, the lack of national commitments led to confusion and resentment in the Solar Sunrise case, especially when U.S. personnel became intensely involved in the Israeli investigative and judicial processes.[42] In spite of encountering difficulties like these, the U.S. and other states were no better prepared when the "I Love You" virus was propagated from a state where deliberate computer attacks were not even illegal.

Even states with advanced economies, and heavily reliant on information technology, have failed to take steps necessary to protect themselves and others from attacks, thereby becoming weak links in the chain of security, or places where criminals and terrorists are able to attack other states with impunity. In his keynote presentation at the Stanford Conference, Raisuke Miyawaki, chairman of Ochanomizu Associates in Tokyo, explained how and why Japan had failed to take Internet security seriously, and the risks this created for Japan's economy and for users worldwide:

> The ease with which the origins of cyber attacks can be hidden, and the fact that cyber attacks on one nation can come from anywhere on the globe, mean that cyber crime and cyber terrorism are truly international threats. And Japan's relatively lax cyber defenses mean that Japan is a potentially weak link in the global economic and

[42] Boaz Gutman, "Constraints on Cooperation," Presentation, at the Stanford Conference, December 7, 1999, pp. 1–3. Michael Vatis, director of the FBI's National Infrastructure Protection Center, testified on July 26, 2000, before the Subcommittee on Government Management, Information, and Technology of the Committee on Government Reform of the U.S. House of Representatives that the lack of laws "that specifically criminalize computer crimes" undercuts investigations in foreign countries. "This means that those countries often lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist us when evidence might be located in those countries." "Computer Security: Cyber Attacks—A War Without Borders," available at 〈*http://www.house.gov/reform/gmit/hearings/2000hearings/000726cybersecurity/000726h.htm*〉.

> security architecture in the event of a major cyber crime, cyber terrorist, or cyber military attack on Japan.[43]

Miyawaki reviewed the rapid increase in illegal network access cases in Japan, as well as several unexplained or unsolved incidents involving break-ins at the national computer research centers, a shutdown of parts of Japan Railway's system in Tokyo, and several shutdowns of the Tokyo Stock Exchange, all caused by computer problems of unknown origin:

> The uncertainty surrounding many of these incidents is troubling. When such network systems crash, they are restored by the company that installed the system, and the problem is not examined by a third party with a special interest in cyber security. Also, unless the crash affects an ATM or other highly visible network that affects customers or everyday citizens, companies don't publicize their computer problems—and, it is said, there are many such incidents that companies don't publicize.[44]

The program Miyawaki recommends to deal with Japan's cybersecurity deficiencies includes the passage of laws making unauthorized access to computer networks illegal (adopted in 1999) and authorizing wiretapping in computer cases (effective August 2000). He also supports Japan's increased involvement in the private-sector and voluntary government programs under way. At the Stanford Conference, he stressed the need for international cooperation, through harmonization of laws and technical issues, emergency response mechanisms, and intelligence sharing. He concluded that, to act effectively against the growing cyber threats, states must in effect form a cyber-defense alliance:

> The goals and tactics and behavior of cyber rogue nations, cyber criminals, and cyber terrorists are threats to all the world's nations. We of the world's leading democratic nations must examine what

[43] Raisuke Miyawaki, "International Cooperation to Combat Cyber Crime and Cyber Terrorism," keynote presentation, at the Stanford Conference, December 7, 1999, p. 2.

[44] Ibid., p. 6.

> has helped us work successfully together in the past, and take lessons from that in preparing for the new era of cyber crime and cyber warfare. Perhaps, we must even create a technologically linked "cyber-defense alliance." And as in so many other matters, the day-to-day sharing of intelligence and information on cyber-security, and the steady building of trust between nations and national officials, will be the bedrock on which international cooperation against cyber crime and cyber terrorism must be built.[45]

The pertinence of Miyawaki's warnings about Japan's vulnerability was fully borne out in January 2000, when a series of humiliating raids on government websites by hackers prompted emergency conditions.[46] His insights are universally applicable.

Vulnerability of Existing Programs

Several participants at the Stanford Conference observed that current computer systems are inherently vulnerable. Robert E. Kahn, president of the Corporation for National Research Initiatives (CNRI), explained that existing systems are unstable and subject to spontaneous failure, even as they are increasingly relied upon for sensitive functions, requiring ever higher levels of complexity.[47] SRI's Peter G. Neumann believes that the unreliability of current technology is by far the greatest danger to cyber security.[48] Vulnerabilities are regularly exploited by hackers and other criminals, and the widespread dominance of highly vulnerable Microsoft programs and services has created a sit-

[45] Ibid., p. 11.

[46] See, e.g., "Hackers Break Into Japan Government," *New York Times on the Web/Breaking News from Associated Press*, January 25, 2000, reported at 〈*http://www.nytimes.com/aponline/i/AP-Japan-Hackers.html*〉; "Japan Calls Emergency Meeting as Hackers Hit Again," *Yahoo! News/Associated Press*, January 26, 2000, at 〈*http://dailynews.yahoo.com/h/nm/20000126/wr/japan_hackers.html*〉; "Japan Moves to Halt Hackers," *New York Times on the Web/Breaking News from Associated Press*, January 28, 2000, reported at 〈*http://www.nytimes.com/aponline/i/AP-Japan-Hackers.html*〉.

[47] See Kahn and Lukasik, "Fighting Cyber Crime and Terrorism," p. 15.

[48] See Peter G. Neumann, "Information System Adversities and Risks," pp. 1, 2, 3.

uation of grave risk.[49] Most software designers, concentrating on satisfying customers seeking greater ease of use and functions requiring greater complexity, regard reliability and security as secondary matters. Enhanced security in cyber systems requires enhanced reliability and stability, not merely quick-fixes in which vulnerabilities to specific types of attacks are eliminiated on a case-by-case basis through design modifications.

The vulnerability of the information infrastructure also stems from the insufficiency of current security measures. The costly "I Love You" virus was "a relatively simple Visual Basic script" that operated much like the "Melissa" virus of the year before, according to Michael J. Miller of *PC Magazine:* "Melissa was enough of a warning. We shouldn't be going through this again."[50] Microsoft provided a fix for the "Melissa" virus, but since it did not change the components targeted by "Melissa," it was still relatively easy to run scripts affecting the settings in Microsoft's widely used Outlook, Outlook Express, Exchange, and Windows. Microsoft left these components unchanged for the same reasons they were designed to be accessible: "convenience for users and letting corporations create complex scripts that tie Outlook together with other Microsoft applications." As Miller points out, while anti-virus makers found the "I Love You" virus and came up with a fix "fairly quickly," this was "not good enough in this era of Internet time. By the time the virus definitions were ready, the virus had already spread. The anti-virus makers must come up with a more generic way of blocking suspicious-looking scripts before they've spread all over the world."[51] Miller also observes how many computer users have failed to implement even the limited security measures that are available for their protection, creating dangers not only for them-

[49] See Charles Piller, "The Cutting Edge: Focus on Technology Innovation—Ubiquitousness of Microsoft Opens Window to Trouble," *Los Angeles Times*, June 5, 2000, p. C-1, available at 2000 WL 2247689.

[50] See Michael J. Miller, "Forward Thinking," *PC Magazine from ZD Wire*, June 27, 2000, available at 2000 WL 18128008.

[51] Ibid.

selves, but also for others, from attacks designed to exploit their inadequate protections.[52]

"Cultural" Vulnerabilities

A subtle aspect of the "culture" of businesses that operate in cyber space is their reluctance to cooperate openly in efforts to suppress cyber crime. The business sector, as Donn B. Parker of Atomic Tangerine (a spin-off of SRI International) explained in his submission to the Stanford Conference, although increasingly reliant on cyber commerce and support, has significantly different incentives from law enforcement with regard to the handling of cyber crime, and consequently with respect to the sharing of information concerning such crime:

> Security is a fundamentally different issue for business than it is for government because the goals of business and government are fundamentally different. Business survives and grows by managing risks, including security risks, to achieve profit and productivity and views security as a necessary enabler to achieve its goals. Security is balanced with other objectives and made as transparent as possible to avoid interfering with or constraining these objectives. Greater security is often promoted and implemented in businesses when it is needed to meet customer expectations or regulator requirements, when losses are occurring, or in attempts to meet standards of due care to avoid negligence. Competing businesses have hidden agendas and sensitive security and loss experience information that would cause them harm if revealed. Business organization public affairs experts reveal cyber crime and security information to the public only when necessary and beneficial under controlled, well-timed circumstances that minimize the negative impact on business objectives.
>
> Governments, and especially military and law enforcement departments, in contrast to business, have security as their goal, and it

[52] Home and university computers are commonly left easily accessible to infiltration and attack. See "Hackers Had Access to Home Computers," *New York Times on the Web/Breaking News from Associated Press*, June 9, 2000, reported at ⟨*http://www.nytimes.com/aponline/a/AP-Hacker-Attack.html*⟩.

> is enforced by law and motivated by significant rewards and penalties. Legislatures, watchdog groups, and news media discover and publicly report losses and security failures within governments, and incidents are vigorously prosecuted. The relationship between business and government organizations is not on a level playing field. Businesses are allowed to fail; governments are not. Governments have hidden agendas that include criminal investigations of businesses and their staffs. Governments may be sued only with their consent. Many government people are sworn officers of the law, have security clearances, and must keep their crime-fighting activities and intent secret.
>
> Governments also have the duty to protect their indigenous infrastructure businesses in the support of commerce and national security and are often frustrated in their efforts to assist reluctant businesses in achieving more effective security. For example, businesses learn from experience that reporting a suspected high-tech crime to law enforcers may result in taking great amounts of valuable employees' time away from business goals to assist in gathering evidence, giving depositions, and acting as witnesses in court appearances.[53]

As Parker concludes, "It is necessary to understand the cultures of businesses and governments to achieve effective security information-sharing and usage among them."[54]

One clear implication of Parker's insights is that cooperation between private and public cyber security experts should occur through voluntary affiliations of businesses, at the national and international level.[55] Parker noted several such efforts, including the International Information Integrity Institute (I-4) and the Information Security Forum (ISF), which serve the information security staffs of many of the world's largest corporations and several governments. Significantly, many of these organizations include present and former government officials, including former law enforcement personnel, who participate

[53] Donn B. Parker, "Sharing Infrastructures' Cyber Crime Intelligence," paper submitted to the Stanford Conference, December 6–7, 1999, pp. 2–4.

[54] Ibid., p. 5.

[55] See the discussion of clearinghouses for such cooperation in Chap. 4 of this volume.

in what Parker observes is in effect an "old boys network" and have a high degree of mutual trust. In addition, other more explicit alliances have been developed between business and government.[56] Parker considers these groups—especially those providing informal exchanges—as the most effective vehicles available for partly overcoming the conflicting interests between businesses and governments, which otherwise limit the likelihood of robust cooperation. He believes they should be allowed to evolve internationally, as a supplement to more formal methods of communication:

> The informal method partly solves or at least sorts out the international dichotomy problem of global businesses interacting with national governments' entities. It provides a means for citizens of each country that are employed by international infrastructure businesses to interact with their own governments that may, in turn, share the information obtained with other governments.[57]

The reluctance of private-sector cyber users to cooperate with governments also suggests that governments cannot responsibly expect the private sector to solve the cyber security problem. Speeches and congressional testimony by U.S. Attorney General Janet Reno and FBI Director Louis J. Freeh called upon businesses for assistance in dealing with cyber crime.[58] The response of the Internet Alliance,

[56] The FBI's Computer Investigations and Infrastructure Threat Assessment Center (CITAC) has joined InfraGard, a business-controlled organization that plans to have fifty chapters throughout the U.S., one in each area served by an FBI field office. The U.S. Treasury Department is cooperating with the private Financial Services Information Sharing and Analysis Center (FS-ISAC), established and operated for U.S.-licensed banks and U.S.-regulated financial firms. Other efforts include cooperation by the U.S. Department of Commerce and the Critical Infrastructure Assurance Office with the power industry.

[57] Parker, "Sharing Infrastructures' Cyber Crime Intelligence," p. 19.

[58] See, e.g., Remarks of Attorney General Janet Reno to the National Association of Attorneys General, January 10, 2000, available at 〈*http://www.usdoj.gov/ag/speeches/*〉; U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS) materials, including "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet" (March 2000), available at 〈*http://www.usdoj.gov/criminal/cybercrime/*〉; "Statement of Louis J. Freeh, Director, Fed-

among others, makes clear that the private sector will reject any effort to overreach and enlist businesses in law enforcement.[59] Businesses will cooperate, but the private sector cannot be expected to perform roles traditionally performed by law enforcement.

The cyber world's culture in fact includes a very significant element of users and participants who strongly oppose virtually any form of government activity. As Stephen J. Lukasik explains below in Chapter 4, the Internet is largely fashioned and run by private-sector experts, some of whom look upon a government role in creating standards mandating or enabling cooperation in law enforcement as a cure more dangerous than the disease of cyber crime.[60] Even as established an organization as the Internet Alliance, composed of representatives from large and powerful cyber and cyber-related businesses such as AOL, AT&T, eBay, Microsoft, Netscape, and Prodigy, has argued that all transnational efforts to control cyber crime should be based on *voluntary* cooperation.[61] In testimony before Congress, businesses have emphasized what Congress should *not* require:

> We must not pass laws of dubious enforceability, risking erosion of the public's confidence in law enforcement and in the Internet. We must resist overreaching, even in the name of security, and make certain that constitutional and statutory protections in the investi-

eral Bureau of Investigation, Before the U.S. Senate Committee on Appropriations, Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies," *Hearing on Cybercrime*, February 16, 2000, available at ⟨*http://www.senate.gov/~appropriations/commerce/freehcyber.html*⟩.

[59] See "Testimony of Jeff B. Richards, Executive Director of the Internet Alliance, Before the U.S. Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and Judiciary," *Hearing on Cybercrime*, February 16, 2000, available at ⟨*http://www.senate.gov/~appropriations/commerce/richards 00.html*⟩.

[60] See, e.g., K. C. Claffy, "Traffic Observation in a Stateless Data Networking Environment," presentation at the Stanford Conference, December 7, 1999, available at ⟨*http://www.caida.org/outreach/presentations/Crisp9912/*⟩.

[61] See, e.g., the materials posted at ⟨*http://www.internetalliance.org/policy/index.html*⟩.

> gation and prosecution of Internet crimes are observed. . . . [I]ndustry cannot and must not be made an agent of law enforcement.[62]

The notion that voluntary activity alone can create adequate security for cyber activities is simply untenable. First, it is likely that at the national level cyber crime would be even more prevalent and costly had the U.S. government left the area unpoliced; the domestic laws so far adopted that make cyber attacks criminal have at least provided a vehicle by which to arrest—and thereby to stop, punish, and deter—cyber attacks designed to steal, defraud, and destroy.[63] The great majority of users—commercial, educational, individual—favor such laws. Effective government on the international level also depends on adopting laws setting universal standards for misconduct, authorizing investigatory cooperation and extradition, and developing and standardizing technologically advanced methods for detecting, blocking, tracking, and deterring prohibited conduct.

A much broader attack on the regulation of cyber space than that advanced by the business community is based on the notion that cyber space cannot or, in any event, should not be regulated by government. John Perry Barlow's claim in "A Declaration of the Independence of Cyberspace" is that cyber space is "an act of nature," based on collective actions, and beyond the borders of any state.[64] This philosophical effort has been supplemented with legal arguments based on a claimed lack of jurisdiction to regulate cyber space. Both the philosophical and the legal claims are thoroughly addressed by Neil W. Netanel, who explains how "courts and legislators have increasingly applied real world, state promulgated law to cyberspace activity, steadily constricting the domain of semiautonomous cyberspace rulemaking," and why these developments, in principle, reflect sound results based on tradi-

[62] "Testimony of Jeff B. Richards, Executive Director of the Internet Alliance," available at ⟨*http://www.senate.gov/~appropriations/commerce/richards 00.html*⟩.

[63] See, e.g., 18 U.S.C. § 1030, "Fraud and related activity in connection with computers."

[64] See ⟨*http://www.eff.org/~barlow/Declaration-Final.html*⟩.

tional liberal democratic theory.[65] Legislators and courts are rapidly coming to regard cyber activities as analogous to other activities already regarded as permitting prescription, investigation, and enforcement on any of the traditional bases for legal regulation.[66]

Resistance to government involvement in cyber regulation is not, however, entirely based on anarchistic preferences or paranoid fantasies; U.S. government actions have undermined trust and strengthened the case for purely voluntary initiatives. The U.S. government has, for example, exerted much effort in attempting to restrict the effectiveness and distribution of advanced encryption, though encryption is widely regarded as one of the most effective tools available for the protection of cyber security and privacy.[67] When the government appeared to have lost its battle to prevent the free transfer and use of encryption, it tried to convince Congress, and later the Internet Engineering Task Force (IETF)—which establishes voluntary standards for Internet Protocols (IPs)—to include "trap doors" in computer security programs so as to enable the government to pursue criminal investigations more easily. The IETF refused to do so.[68] The implementation

[65] See Neil Weinstock Netanel, "Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory, *California Law Review* 88, no. 395 (March 2000): 2–4.

[66] See, e.g., *Governor of Brixton Prison and Another, Ex Parte Levin*, 3 W.L.R. 657 (Q.B. 1996), *aff'd* 1 Crim. App. 22 (1997). See also Jack L. Goldsmith, "Against Cyberanarchy," *University of Chicago Law Review* 65 (1998): 1199.

[67] See Michael R. Arkfeld, "E-Mail—Revisiting Security Issues," *Arizona Attorney* 27, no. 12 (Aug./Sept. 2000): "Encryption [is] a useful method to insure privacy in e-mail transmissions. Encrypting data sent over the Internet renders that message unbreakable, except by the most sophisticated of computer decrypting programs. Encrypted files are 'nearly impossible to break.'"

[68] See, e.g., "IETF Rejects FBI Pressure to Allow Network Wiretaps," *Network News*, February 16, 2000, available at 2000 WL 7833204. See also Amy Zuckerman, "Task Force Tackles Internet Standards," *Journal of Commerce*, April 19, 2000, available at 2000 WL 4187332: "The IETF isn't beholden to any country." Some additional changes sought by the U.S. government may, however, be entirely appropriate and consistent with existing authority. See "Statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Before the Senate Committee on Judiciary" (seeking enhancement of "the ability of law enforcement at the federal, state, and local level to address the burgeoning load

of a search engine injudiciously called "Carnivore " enhanced distrust, although the system seems potentially consistent with legal standards.[69]

Distrust on the international level has been generated by the COE's Draft Convention on Cyber-Crime, the most recent version of which (at the time of this writing) was released on November 19, 2000.[70] This draft—the twenty-fourth since the exercise was initiated—includes coverage of copyright offenses, despite the lack of international consensus on the scope and forms of protection of the many types of works potentially covered. The draft also specifies the types of cooperation that may be required under it, not only from States Parties, but also from Internet Service Providers (ISPs) and other entities and individuals. Among other things, ISPs may be required to conduct real-time surveillance of customers (an earlier draft had required them to store at least forty days of customer data), and all entities and individuals could be required to provide passwords (an earlier draft would have used technology to identify each computer on the Internet). Criticisms of the COE's draft convention, which has been substantially revised in recent months, are in many respects unwarranted, and fail

of computer forensics"), available at ⟨*http://www.senate.gov/judiciary/52520mav.htm*⟩.

[69] See "Congress Probes FBI E-Mail Snooping Device," *Palo Alto Daily News*, July 25, 2000, p. 10: "Lawmakers of both parties grilled FBI officials . . . over the bureau's use of 'Carnivore,' a device designed to monitor and capture e-mail messages in a criminal investigation." See also "Justice Dept. Seeks Carnivore Review," *New York Times on the Web/Breaking News from Associated Press*, August 24, 2000, reported at ⟨*http://www.nytimes.com/aponline/w/AP-Carnivore.html*⟩; Will Rodger, "'Carnivore' Unlikely to be Validated," *USA Today*, September 5, 2000, available at ⟨*http://www.usatoday.com*⟩. For contrary views, see Ted Bridis, "FBI Gets Web Guru Cerf's Support for Carnivore," *Wall Street Journal*, September 7, 2000, B8: "The Federal Bureau of Investigation has largely won over a crucial ally, technology pioneer Vinton Cerf, in its bid to defend the use of its Carnivore Internet surveillance system"; Ted Bridis and Neil King, Jr., "Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI," *Wall Street Journal*, July 20, 2000, A28; Bruce D. Berkowitz, "'Carnivore' Won't Devour Cyber-Privacy," *Wall Street Journal*, July 19, 2000, p. A22.

[70] See "Draft Convention on Cyber-Crime," released for public discussion on November 19, 2000, available at ⟨*http://conventions.coe.int/treaty/en/projets/cybercrime24.htm*⟩.

to take into account that all the measures it proposes are "subject to the conditions and safeguards provided for under the domestic law of the Party concerned, with due regard for the adequate protection of human rights and, where applicable, the proportionality of the measure to the nature and circumstances of the offence."[71] But the COE's effort has evoked negative reactions because of its scope and because it seeks to establish standards without allowing for an open process in which the private sector is able fully to participate.

Widespread distrust of the intentions of commercial entities and merchandising groups with regard to privacy also exists among experts and consumers. Commercial entities and service providers have unilaterally developed and used intrusive software and practices that fail to inform consumers adequately or to provide effective methods for opting out of information-collecting programs.[72] Congress and the Federal Trade Commission (FTC) are considering restrictions on merchandising and consumer tracking aimed at protecting privacy.[73] Finally, private-sector decisions to maintain proprietary systems and programs designed for user convenience and accessibility rather than for security are themselves a root cause of cyber vulnerability; the private sector could greatly enhance cyber security by reordering design priorities, without any government involvement.

An enhanced government role need not, however, be one that requires significantly greater domestic powers or more intrusive mea-

[71] See ibid., art. 14, § 2.

[72] "TRUSTe, a privacy advocate organization that runs a privacy seal-of-approval program for retail Web sites and shows companies how to write effective privacy policies, itself has tracked users with means not mentioned in its own policy." See "Group: Web Agency Tracks Users," *New York Times on the Web/Breaking News from Associated Press*, August 24, 2000, which was reported at ⟨*http://www.nytimes.com/aponline/w/AP-Online-Privacy.html*⟩.

[73] See Brian Krebs, "Senate Considers Stronger Anti-Cybercrime Measures," *Newsbytes News Network*, May 25, 2000, reporting on proposed legislation to permit consumers to opt out of programs that collect and use personal information, and on a Federal Trade Commission proposal to allow consumers to view and change any personal information already collected on them), available at 2000 WL 21177763.

sures;[74] rather, the need is for international cooperation to create common standards and practices. In attempting to satisfy these objectives, it is imperative to take into account the legitimate concerns of those who seek to avoid conferring inappropriate or unnecessary powers on governments to regulate and to intrude upon cyber systems, to preserve as far as practicable private-sector control of this uniquely productive and dynamic sector, and to avoid impinging upon national security interests and activities. As Lawrence Lessig has explained, it is illusory to believe that the cyber world cannot be regulated, and to expect that it will not be regulated, for purposes of facilitating commerce, enhancing security, and—one hopes—protecting freedom and privacy.[75] Regulatory power exists in the "code" that governs all cyber activities. But the scope of regulation will depend on the measures adopted, and it is on that front that the battle over the future of the cyber world must be fought.

5. Fashioning a Solution

A program to deal with cyber crime should be based on its characteristics and be limited to the steps needed to address identified weaknesses. The Stanford Conference made clear to many of us the need

[74] See, e.g., Jennifer Jones, "U.S. Cyberattack Protection Plan Draws Criticism," *CNN.com*, February 3, 2000, reporting on "red flags" raised in objection by the Electronic Privacy Information Center (EPIC), among others, to Clinton Administration proposals for safeguarding critical systems against cyber attacks, which was reported at ⟨*http://cnn.com/2000/TEC...cyberprotection.crit.idg.index.html*⟩. Enhanced national penalties, and greater police powers for the FBI or other national police agencies, seem unlikely to affect, let alone solve, the rash of ever costlier cyber attacks. Longer jail terms in the U.S., for example, as recent legislation proposes, could have a bearing on the conduct only of individuals likely to be subjected to U.S. law. As a reaction to the "I Love You" virus, for example, raising penalties would be a pointless gesture, since Philippine attackers are immune from the application of U.S. law. Only when the U.S. and Philippine governments agree to make cyber attacks crimes for which extradition is promised by both states will the possibility of an enhanced U.S. penalty become even conceivably relevant.

[75] See Lawrence Lessig, *Code: And Other Laws of Cyberspace* (New York: Basic Books, 1999).

for some form of international cooperation. Our effort here is to determine what sort of cooperation is called for, and how best to provide it.

First, the transnational nature of cyber crime calls for a transnational response. The actions of individual states are insufficient. Affected states need to agree on the kinds of conduct that should be proscribed and adopt laws making such conduct criminal. Chapter 2 of this volume examines the considerable extent to which an international consensus exists for prohibiting most forms of attacks on computers and computer networks. Considerable consensus also exists on problems of regulating some conventional crimes in which computers are used, including cyber-related child pornography; but as Chapter 6 points out, on many such crimes major differences of political outlook would make a universal agreement impossible. Still, the exclusion of many conventional crimes involving the use of computers from an international agreement is less important than ensuring comprehensive coverage of harmful conduct aimed at computers and their operation, with a commitment to impose substantial penalties.

In addition to ensuring universal condemnation of serious forms of misconduct, any effective system for punishing cyber crime will require the full range of cooperation afforded by states to each other in mutual legal assistance and extradition treaties. The nature of cyber crime also requires national commitments to undertake special efforts to search for, secure, and preserve usable evidence. The speed with which cyber-related evidence can be lost, and the frequency with which it will be located in foreign jurisdictions, makes it necessary to have the consent of states in advance to some forms of searches that reach into their territories, as well as agreements to assist in seizing equipment and other assets and to provide usable evidence and other forms of cooperation. It is insufficient, moreover, for states merely to agree to perform conventional services for each other. They will have to be prepared to implement technologically adequate measures, as these are developed. Participants at the Stanford Conference described efforts under way to enhance the capacity of users, providers, investigators, and prosecutors to deal with the challenges posed by cyber attacks (summarized below in Chapter 4).

Securing agreement from all states connected to the international information infrastructure for these far-reaching forms of cooperation will certainly be more difficult than securing agreement on the conduct to be proscribed. No multilateral consensus yet exists on providing legal assistance and extradition in cyber cases. States must be convinced that such cooperation is in their best interests, as in the areas of civil aviation (discussed in Chapter 3), international banking, money laundering, and narcotics. To overcome claims or fears of improper extraterritorial activities, states should agree that all measures undertaken in pursuing a cyber investigation will be performed in a manner consistent with the law of the state that is asked to perform such services. To overcome claims or fears that cyber investigations or prosecutions could compromise domestic constitutional protections (see Chapter 5), no state should be required by the international commitments it undertakes to compromise its national standards of conduct. In addition, some states, owing to the so-called "cyber divide," will be unable to provide the assistance required by an international agreement. It is very much in the interests of all states to guard against "weak links" in cyber crime enforcement (that could be exploited by attackers). States should agree to a program to assist those states with legitimate needs in this regard, as international agencies do in a number of other arenas requiring technological expertise.

Because cyber systems and programs are designed with efficiency and ease of use rather than security as the primary objective, states should consider adopting technological measures that go beyond investigative cooperation. Technological breakthroughs (of the sorts discussed in Chapter 4) to enhance protection against, and to improve investigation and prosecution of, cyber crimes should be encouraged and widely implemented. To achieve such cooperation will require overcoming the antiregulatory perspectives of private-sector participants who have built and continue to develop the information infrastructure. One necessary response to this resistance is to build private-sector control into the process of developing solutions and formulating standards and practices for enhancing cyber security. This is one of the guiding principles used in designing the multilateral convention presented below in Chapter 6. In addition, the proposed convention seeks to ensure not only that national standards of state conduct related to human rights are preserved, but also that States Parties will provide certain minimum due process rights in the arrest, charging, prosecution, and extradition of suspects, analogous to protections widely regarded as required by international law. Finally, the Draft Convention explicitly makes it inapplicable to national security activities. U.S. officials are justifiably concerned that an international agreement might lead to unwarranted restrictions on defense-related activities. This possibility can be successfully averted, however, as in other treaties potentially bearing upon national security.

A program based on these principles and proposals should eventually overcome resistance to a multilateral convention to deal with cyber crime and terrorism. Escalating damage and the inadequacy of current efforts are increasing the pressure on governments—and through them on ISPs, major companies, and private standard-setting bodies—to respond effectively. Efforts by governments reacting to recent major attacks have focused on seeking (or in the case of legislators offering) new powers, such as stiffer sentences, the right to arrest and/or search without prior judicial approval, and other inadequate and damaging measures.[76] Knowledgeable legislators and industry leaders should eventually turn to more useful and appropriate options.

[76] See "Statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Before the Senate Committee on Judiciary" (supporting, among other things, "provisions that would increase the penalties available for those who are convicted"), available at 〈*http://www.senate.gov/judiciary/52520mav.htm*〉. See also Brian Krebs, "Senate Considers Stronger Anti-Cybercrime Measures," reporting on S. 2448, proposed by Senate Judiciary Committee Chairman Orrin Hatch (R-Utah) and Senator Charles Schumer (D-NY), which "would remove the $5,000 damage threshold for prosecuting federal cybercrimes," and noting FBI efforts to more easily obtain "trap and trace" wiretaps "across many different states," available at 2000 WL 21177763.

Apart from the dangers of increasing police powers, relying on prosecutors to plan and implement solutions in a highly technical area in which private control is regarded as a substantial advantage may well be ineffective even in satisfying the need for better security.[77]

Those who support adoption of a multilateral approach to deal with this quintessentially transnational problem must be encouraged by the fact that states have consistently adopted multilateral solutions to deal with technologies that affect populations across national boundaries. As technology advances, new technologies with transnational impact that require transnational controls have repeatedly led to multilateral arrangements; agencies have been created to deal with such international areas as air travel, shipping, and telecommunications. Transnational needs have demanded transnational solutions, which have been satisfied through international agreements on principles, standards, and practices, often developed and proposed by specialized international agencies. States make such arrangements based not upon ideological considerations but on considerations of safety, productivity, and efficiency. They have done so, moreover, with no sacrifice of national sovereignty, and almost entirely on the basis

[77] It may, in fact, be a mistake to continue to place primary responsibility for coping with cyber crime within the scope of agencies oriented toward criminal investigations, such as the FBI. Prosecutorial agencies are concerned with developing information for their own use, and tracing and capturing criminals. They are not necessarily going to use information to warn the public of attacks or to develop policy and/or technological solutions aimed at making successful attacks less likely. The U.S. General Accounting Office (GAO) report on the NIPC's response to the "I Love You" virus noted that the agency (which is part of the FBI) waited hours after learning of the virus to notify the public, by which time most companies had been infected. See "Statement of Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems Accounting and Information Management Division, U.S. General Accounting Office, Before the Subcommittee on Financial Institutions, Committee on Banking, Housing, and Urban Affairs, U.S. Senate," *Critical Infrastructure Protection: "I Love You" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, May 18, 2000 (GAO/T-AIMD-00-181), available at ⟨*http://www.gao.gov/*⟩. Furthermore, agencies such as the FBI are unlikely to create systemic recommendations, since they are not immediately concerned with relevant private-sector experts or with the internal capacities to develop such plans.

of consensus decisions determined by both self-interest and reciprocity.

The information infrastructure faces analogous challenges. Its security and efficiency will be materially increased through international implementation of principles, standards, and practices specifically designed for this field of activity. The optimum manner of achieving these objectives in this particular field is a multilateral treaty with the necessary commitments to cooperate in investigating and prosecuting an agreed range of conduct, and an international agency with authority to accomplish (through measures analogous to those widely in use by other agencies; see Chapter 6) the legal and technological objectives essential to create a more secure cyber world.