Backgrounder

Published by The Heritage Foundation

No. 2105
February 8, 2008

Combating Enemies Online: State-Sponsored and Terrorist Use of the Internet

James Jay Carafano, Ph.D., and Richard Weitz, Ph.D.

Even before the terrorist attacks of September 11, 2001, security experts were becoming increasingly concerned about the vulnerability of U.S. computer systems and associated infrastructure. The 9/11 attacks amplified these concerns.

Less attention, however, has been paid to state sponsors of illicit computer activity, which are increasingly using the Internet to conduct espionage, deny services to domestic and foreign audiences, and influence global opinion. In addition, insufficient focus has been given to how terrorists exploit the Internet as a tool for recruiting, fund raising, propaganda, and intelligence collection and use it to plan, coordinate, and control terrorist operations. Combating these malicious activities on the Internet will require the cooperation of federal entities, as well as friendly and allied countries and the private sector.

Recent cyber initiatives show promise, but a more concerted national effort is required, particularly in acquiring commercial capabilities and services, managing military intelligence and information technology programs, and developing a corps of professional national security practitioners.

Dangers Lurking

In recent years, government and private information networks have increasingly come under attack from a variety of state-sponsored and non-state actors.

State-Sponsored Threats. A widely publicized cyber assault against Estonia in 2007 increased suspicions that adversarial states are using online malicious

Talking Points

- Washington has paid little attention to state sponsors of illicit computer activity, which are increasingly using the Internet to conduct espionage, deny services to domestic and foreign audiences, and influence global opinion.
- Analysts have also documented a steady increase in terrorists' use of the Internet, both as a tool for recruiting, fund raising, propaganda, and intelligence collection and as a tool in planning, coordinating, and controlling terrorist operations.
- The United States is not defenseless in the face of illicit exploitation of computer networks. Both the government and the private sector have developed significant capabilities.
- Effectively combating enemies online will require a concerted national effort, particularly in acquiring commercial capabilities and services, managing military intelligence and information technology programs, and developing a corps of professional national security practitioners.

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/bg2105.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

activity as a tool of national policy. The assault disrupted public and private Estonian information networks with massive denial-of-service attacks. Recent revelations of Chinese cyber-espionage activities against sensitive information networks in the United States, Germany, and other countries have further heightened concerns that the World Wide Web is becoming just another battlefield.[1]

The Estonia attacks targeted the Web sites of banks, telecommunication companies, media outlets, and government agencies, eventually forcing the country to block all foreign Internet traffic.[2] Many Web sites were shut down by denial-of-service attacks, in which the attacker uses thousands of hijacked computers to bombard a Web site with useless information until it is overloaded. For one bank, disruptions in cyberspace resulted in material losses of over $1 million after it was forced to shut down online services.[3] At one point, telephone service for fire and rescue units was suspended for over an hour.[4]

Estonia's defense minister described the attacks as "a national security situation…. It can effectively be compared to when your ports are shut to the sea."[5] The Estonia attacks vividly testify to the disruptive power of a coordinated cyber offensive.

Chinese intentions also give cause for concern. Senior defense analysts believe that China has undertaken a sustained effort to develop information warfare capabilities to achieve "electromagnetic dominance" over the United States and other potential competitors.[6] Security experts believe that the Chinese government orchestrated a sophisticated cyber-espionage effort known as Titan Rain, which downloaded information from hundreds of unclassified defense and civilian networks.[7]

U.S. government information systems are attacked every day from sources within the country and around the world. Some of these intrusions have been extremely serious, compromising security and costing millions of dollars. Penetration of computer networks at the National Defense University proved so pervasive that the university was forced to take the entire computer network offline and install new information system defenses.

In 2007, *Der Spiegel* alleged that Chinese programmers had placed spy software on computers at the Foreign, Economics, and Research and Development Ministries as well as on computers used by the Chancellery office.[8] Such Trojan horse programs can capture data from host computers and transmit the information to external users. The immense scale of the Internet espionage operations suggests that they could not have occurred without the knowledge and at least the tacit support of an official Chinese entity.

Shortly after the *Spiegel* article was published, officials in Britain, France, the United States, and other countries indicated that they had found similar evidence of Chinese cyber-espionage campaigns.[9] This evidence includes media reports of

1. For more on Chinese cyber-espionage, see John J. Tkacik, Jr., "Trojan Dragon: China's Cyber Threat," Heritage Foundation *Backgrounder* No. 2016, February 8, 2008, at *www.heritage.org/Research/AsiaandthePacific/bg2016.cfm*.
2. Peter Finn, "Cyber Assaults on Estonia Typify a New Battle Tactic," *The Washington Post*, May 19, 2007, p. A1, at *www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html* (January 31, 2008), and Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 17, 2007, at *www.guardian.co.uk/russia/article/0,,2081438,00.html* (January 29, 2008).
3. Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 24, 2007, at *www.nytimes.com/2007/05/29/technology/29estonia.html* (January 31, 2008).
4. "Newly Nasty," *The Economist*, May 24, 2007, at *www.economist.com/world/international/displaystory.cfm?story_id=9228757* (January 29, 2008).
5. Landler and Markoff, "Digital Fears Emerge After Data Siege in Estonia."
6. U.S. Department of Defense, Office of the Secretary of Defense, *Military Power of the People's Republic of China: 2007*, 2007, at *www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf* (January 29, 2008).
7. Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, August 25, 2005, p. A1, at *www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html* (January 29, 2008).
8. "Chinesische Trojaner auf PCs im Kanzleramt" (Chinese Trojans in Chancellor Office PCs), *Der Spiegel*, August 25, 2007, at *www.spiegel.de/netzwelt/tech/0,1518,501954,00.html* (January 28, 2008).

cyber penetration of the U.S. Department of Homeland Security (DHS) and U.S. Department of Defense from Chinese-language Web sites.[10]

Another concern is the surety of original software and computer components. In two recent reports, the Defense Science Board has warned about the potential vulnerability to intrusion, malicious activity, and exploitation via malicious software and semiconductor components.[11]

Non-State Threats. Analysts have also documented a steady increase in terrorists' use of the Internet.[12] In addition, transnational criminal organizations routinely conduct cyber operations, including identity theft and fraud.

Internet Exploitation. One comprehensive survey has identified specific ways that terrorists employ the Internet.[13] They use the Internet to:

- *Wage psychological warfare by spreading disinformation*, delivering threats to instill fear and helplessness, and disseminating horrific images. For example, the grisly murder of Daniel Pearl was videotaped by his captors and posted on several terrorist Web sites.
- *Create publicity and spread propaganda.*
- *Gather intelligence.* Details about potential targets—such as transportation facilities, nuclear power plants, public buildings, ports, and airports—and even counterterrorism measures are available online. For example, the DHS maintains a password-protected online site called Tripwire, which provides information on how to counter improvised explosive devices (IEDs).
- *Fundraise.* Many Islamic charitable organizations allow users to make a *zakat* contribution online. Some terrorist organizations use front companies and charitable organizations under their control to receive such donations.
- *Recruit and mobilize supporters* through chat rooms, cybercafés, and bulletin boards.
- *Communicate and coordinate with operatives and supporters.* Two terrorist cells in Florida and Canada, which were recently disrupted, passed messages via the Internet.
- *Share information*, such as how to manufacture and use weapons, including bomb-making techniques.
- *Plan attacks.* To preserve their anonymity, the 9/11 attackers used the public Internet services and sent messages via free Web-based e-mail accounts.

Al-Qaeda and other transnational terrorist networks rely heavily on the Internet to communicate with dispersed operatives. The organization's messages appear on approximately 6,000 Web sites.[14] As-Sahab Institute, al-Qaeda's media component, has released a slew of videos—about one every three days since the beginning of 2007—featuring Osama bin Laden and other terrorist leaders. Observers have been impressed by both the quantity of these releases and the institute's use of the latest commercial computer software and hardware in producing and distributing them.[15]

9. Demetri Sevastopulo and Richard McGregor, "Chinese Hacked into Pentagon," *Financial Times*, September 3, 2007, at *www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html* (January 31, 2008).
10. Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *The Washington Post*, September 24, 2007, p. A1, at *www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html* (January 31, 2008).
11. Defense Science Board, *Mission Impact of Foreign Influence on DoD Software*, September 2007, at *www.acq.osd.mil/dsb/reports/2007-09-Mission_Impact_of_Foreign_Influence_on_DoD_Software.pdf* (January 31, 2008), and *High Performance Microchip Supply*, February 2005, at *www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf* (January 31, 2008).
12. For example, see Jim Melnick, "The Cyberwar Against the United States," *The Boston Globe*, August 19, 2007, at *www.boston.com/news/globe/editorial_opinion/oped/articles/2007/08/19/the_cyberwar_against_the_united_states* (January 31, 2008).
13. Gabriel Weimann, "www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace *Special Report* No. 116, March 2004, at *www.usip.org/pubs/specialreports/sr116.pdf* (January 29, 2008).
14. Arnaud de Borchgrave, "Al Qaeda on the Ropes?" *The Washington Times*, September 28, 2007, at *www.washingtontimes.com/article/20070928/COMMENTARY/109280001/1012/commentary* (January 31, 2008).
15. Shaun Waterman, "Al Qaeda Tapes Grow in Number, Expertise," *The Washington Times*, September 24, 2007, at *www.washingtontimes.com/apps/pbcs.dll/article?AID=/20070924/FOREIGN/109240065/1001* (January 31, 2008).

The Internet offers terrorists certain advantages over more traditional means of communication and operation:

- Easy access,
- Little government control,
- Potentially enormous domestic and foreign audiences,
- Anonymous communications,
- Rapid information exchanges,
- Low cost,
- Multimedia platforms, and
- The ability to influence other mass media that rely on the Internet for stories.[16]

The Internet also gives terrorists tremendous operational flexibility. When extremist Web sites have been identified, hacked, or shut down by Internet service providers (ISPs), the terrorists have turned to chat rooms and message boards for communication. Their Web sites commonly disappear from and return to the Web. Al-Qaeda operatives post their messages and videos on Islamist forums.[17]

Non-State Cyber Attacks. Islamist hackers have promoted the tactic of "electronic jihad," attacking "enemy" Web sites to harm the enemy's morale and economic and military infrastructure. Many Islamist Web sites host forums that discuss how to conduct such Web-based offensives.[18] The Web is a target-rich environment. The Department of Defense alone has 3.5 million computers and 35 internal networks located in 65 countries, many of which depend on commercial systems.[19]

Propaganda and Fundraising. One of the most troubling developments has been the use of the Internet by Sunni insurgent groups in Iraq. These groups use the Web to conduct media campaigns by distributing videos, online magazines, blogs, video clips, full-length films, and online television programs. According at an authoritative study by Radio Free Europe/Radio Liberty's Arabic Language Service:

> [These products are] undermining the authority of the Iraqi government, demonizing coalition forces, fomenting sectarian strife, glorifying terrorism, and perpetrating falsehoods that obscure accounts of responsible journalists. Insurgent media seek to create an alternate reality to win hearts and minds, and they are having a considerable degree of success.[20]

These products are designed primarily for political activists who are native Arabic speakers and have high-speed Internet connections. The majority of downloads are in the Middle East but outside of Iraq. Insurgent media appear to be most effective in fundraising and influencing "opinion makers," and secondarily as a source of recruiting.[21]

The Response

The over 1 billion users on the Internet include threats to American security. Efforts to combat them have been increased as the danger has grown.

Federal Programs. The U.S. government took some measures before 9/11 to enhance cybersecurity and its capacity to combat malicious activity on the Web, including a 1987 requirement that government personnel protect their computer data and formulation of the first national cybersecurity strategy in 2000. However, strong resistance from civil liberties and privacy groups as well as anemic funding from Congress prevented the establishment of a planned government network to detect intrusions.

16. Weimann, "www.terror.net."
17. Middle East Media Research Institute, "The Enemy Within: Where Are the Islamist/Jihadist Websites Hosted, and What Can Be Done About It?" *Inquiry and Analysis Series* No. 374, July 19, 2007, at *http://memri.org/bin/articles.cgi?Page=archives&Area=ia&ID=IA37407* (January 29, 2008).
18. *Ibid.*
19. "US and China Leaders Thursday Add Cyber Warfare to Agenda Including Trade and Global Warming," *San Francisco Sentinel*, September 5, 2007, at *www.sanfranciscosentinel.com/?p=4759* (January 29, 2008).
20. Daniel Kimmage and Kathleen Ridolfo, *Iraqi Insurgent Media: The War of Images and Ideas*, Radio Free Europe/Radio Liberty *Special Report*, June 2007, p. 4, at *http://realaudio.rferl.org/online/OLPDFfiles/insurgent.pdf* (January 31, 2008).
21. *Ibid.*, p. 62.

After the 9/11 attacks, Washington took additional steps to improve the safety and security of its online information. In 2002, Congress enacted the Federal Information Security Management Act 2002, which requires agencies to develop policies and standards to protect the integrity, confidentiality, and availability of Internet-based information. In February 2003, the Administration released the *National Strategy to Secure Cyberspace*.[22]

Homeland Security. In 2003, DHS, in cooperation with Carnegie Mellon University, created a computer emergency response team (CERT) to coordinate emergency efforts and established an alert system for cyber threats. The US-CERT has also sought to facilitate public–private cybersecurity partnerships, notably by sponsoring the National Cyber Security Summit in December 2003.[7] Today, most responsibility falls under the National Cyber Security Division.

Intelligence Operations. The intelligence community maintains a clandestine technical collection program. Although few operational details are publicly available, intelligence agencies are widely believed to have some capability to penetrate computer systems used by transnational terrorist networks. These efforts include passively intercepting communications to identify cells and determine their activities. Presumably, the intelligence community also has the capacity to disrupt terrorist operations by, for example, denying services, hacking computer programs, and altering terrorist messages.

More is publicly known about the intelligence community's defensive capabilities. Strengthening cybersecurity has been a key objective of the Information Sharing Environment (ISE), a collection of policies, procedures, and technologies that permit the exchange of terrorism information, including intelligence and law enforcement data. The ISE aims to promote a culture of data sharing among its participants to ensure that information is readily available to support their missions. The ISE connects federal, state, local, and tribal governments. It also envisions a critical role for private-sector and foreign actors in sharing information to counter terrorist threats.[23]

Military Responses. The military increasingly envisions cyberspace as a theater of operations. Defense operations range from field activities to strategic campaigns. For example, U.S. forces in Iraq have undertaken operations to suppress insurgent propaganda networks that use the Internet against coalition forces.[24]

At the national level, the U.S. Strategic Command (STRATCOM) has played a role in global cyber operations since its creation in 1992. STRATCOM's Joint Functional Component Command for Network Warfare was established in 2005 and is responsible for working with federal agencies on computer network defense and for planning offensive information warfare. The Director of the Defense Information Systems Agency also heads a Joint Task Force for Global Network Operations.

The military services, particularly the Air Force, have demonstrated an increased interest in cyber operations. The Air Force recently announced the creation of a Cyberspace Command on par with other Air Force major commands to develop information warfare capabilities and doctrine.[25] Lieutenant General Robert Elder, Commander of the 8th Air Force, is helping to set up the new command. He has emphasized the need to "ratchet up our capability" in cyberspace to challenge China's emphasis on information warfare.[26]

This military emphasis on cyberspace does not necessarily translate into protection against the kinds of disruptions experienced in Estonia. The

22. The White House, *The National Strategy to Secure Cyberspace*, February 2003, at *www.whitehouse.gov/pcipb/cyberspace_strategy.pdf* (January 29, 2008).
23. Information Sharing Environment, *Information Sharing Environment Implementation Plan*, November 2006, at *http://ise.gov/docs/ise-impplan-200611.pdf* (January 29, 2008).
24. Jim Michaels, "U.S. Pulls Plug on 6 Al-Qaeda Outlets," *USA Today*, October 5, 2007, at *www.usatoday.com/news/world/iraq/2007-10-04-Mediacenter_N.htm* (January 31, 2008).
25. Mackenzie Eaglen, "The Air Force's Cyber Command: Combating Electronic and Network Threats," Heritage Foundation *WebMemo* No. 1629, September 20, 2007, at *www.heritage.org/Research/NationalSecurity/wm1629.cfm*.
26. "General: China Taking on U.S. in Cyber Arms Race," CNN, June 13, 2007.

Defense Department's policy on cyberwarfare specifically emphasizes protecting the military information network and developing offensive cyberwar capabilities against potential adversaries.[27]

International Cooperation. The attacks against Estonia, a NATO member, have reenergized multinational cyber defense efforts. NATO information specialists have traditionally concentrated on protecting the alliance's own networks, especially those that might support collective military operations. The Estonia incident led NATO to deploy some of its information specialists to provide immediate assistance.[28]

The Estonian CERT was effective in reducing the level of disruption caused by the attacks. By coordinating the work of foreign Internet service providers, local law enforcement, and network managers across the country, the CERT ensured that Estonia's information infrastructure responded in a coordinated manner. Without an empowered and properly funded CERT, the cyber attacks could have lasted much longer and been more disruptive.[29]

However, Estonia's cyber disruption highlighted the need to clarify both international and domestic responses to malicious cyber activities. Member governments are currently studying the question of precisely which conditions would cause such attacks to fall within the alliance's definition of self-defense, requiring a collective NATO response under Article 5 of the North Atlantic Treaty.[30]

NATO is not the only organization demonstrating renewed interest in combating cyber threats. The United Nations, the Council of Europe, the Shanghai Cooperation Organization, and other international bodies have initiated programs aimed at countering information attacks through the Internet, including attacks by terrorist groups.

Public–Private Partnerships. In 2003, the White House issued Homeland Security Presidential Directive 7, which emphasized that "critical infrastructure and key resources provide the essential services that underpin American society."[31] The directive resulted in development of the National Infrastructure Protection Plan (NIPP), which was released in 2006. The NIPP details cooperative strategies for public-sector and private-sector information sharing and network protection.[32]

The NIPP relies on several institutions, particularly Information Sharing and Analysis Centers (ISACs), to facilitate the exchange of information with critical business sectors, such as financial institutions and energy companies. ISACs are established and funded by the private sector, and the data handled by ISACs are provided largely by private-sector participants. ISACs also receive information from other entities, including law enforcement agencies and security associations.[33] In addition to the ISACs, critical business sectors have Sector Coordinating Councils that develop policy recommendations in coordination with government agencies.[34] The NIPP and its associated centers provide the backbone of the DHS cyber effort.

27. Clay Wilson, "Information Operations and Cyberwar: Capabilities and Related Policy Issues," Congressional Research Service *Report for Congress*, updated September 14, 2006, at *www.fas.org/irp/crs/RL31787.pdf* (January 29, 2008).
28. Jim Michaels, "NATO to Study Defense Against Cyberattacks," *USA Today*, June 15, 2007.
29. Ben Arnoldy and Gordon Lubold, "Could US Repel a Cyberattack?" *The Christian Science Monitor*, June 7, 2007, at *www.csmonitor.com/2007/0607/p01s01-usmi.htm* (January 29, 2008).
30. Greg Jaffe, "Gates Urges NATO Ministers to Defend Against Cyber Attacks," *The Wall Street Journal*, June 15, 2007.
31. George W. Bush, "Critical Infrastructure Identification, Prioritization, and Protection," Homeland Security Presidential Directive HSPD-7, December 17, 2003, at *www.whitehouse.gov/news/releases/2003/12/20031217-5.html* (January 29, 2008).
32. U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2006, at *www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf* (January 29, 2008).
33. *Ibid.* ISACs exist for 14 types of critical infrastructures. For a current assessment of their effectiveness, see Eileen R. Larence and David A. Powner, "Critical Infrastructure: Challenges Remain in Protecting Key Sectors," GAO–07–626T, testimony before the Subcommittee on Homeland Security, Committee on Appropriations, U.S. House of Representatives, March 20, 2007, at *www.gao.gov/new.items/d07626t.pdf* (January 29, 2008).
34. U.S. Department of Homeland Security, *National Infrastructure Protection Plan*.

In addition to the strategies outlined by the NIPP, information sharing between government and the private sector receives considerable support from InfraGard, a program established by the FBI in 1996.[35] Originally developed to assist cybercrime investigations, InfraGard facilitates collaboration with law enforcement, business, and academia on a range of security-related issues. InfraGard chapters facilitate information collection, analysis, and training and provide discussion forums to share best practices. InfraGard also provides a secure Web-based communications platform.[36]

Nongovernmental Efforts. Private-sector companies, universities, research centers, and nongovernmental groups have developed capabilities to combat malicious cyber activities and to investigate or disrupt terrorist operations on the Internet. Perhaps the best-known of these groups is the Internet Security Alliance, a collaboration between the Electronic Industries Alliance, a federation of trade associations, and Carnegie Mellon University's CyLab. It was established to provide a forum for information sharing and to generate suggestions for strengthening information security.

Many other organizations and private-sector companies support America's cyber defenses. The University of Arizona has conducted a multi-year project called Dark Web, which attempts to monitor how terrorists use the Internet. The university's Artificial Intelligence Lab has accumulated the world's most extensive database of terrorist-related Web sites—over 500 million pages of messages, images, and videos—and has made it available to the U.S. military and intelligence communities. Some of its sophisticated software exposes social linkages among radical groups and seeks to identify and track individual authors by analyzing their writing styles. This knowledge enables researchers to assess which people are most susceptible to radicalization and which terrorist recruitment messages are most effective. The university recently received a $1.5 million federal grant to concentrate on how extremists use the Internet to teach terrorists how to construct IEDs.[37]

The Middle East Media Research Institute (MEMRI) publicizes extremist messages on the Internet, including terrorist Web sites, discussion forums, and blogs. After MEMRI published a comprehensive survey of Islamist Web sites in 2004, many them were closed down by their hosting ISPs.[38]

After 9/11, the U.S. Military Academy at West Point established a Combating Terrorism Center. Among the center's studies, *The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda*[39] provides a ready guide to commonly used terrorist graphics, symbols, icons, and photographs.

In addition to these efforts, nongovernmental organizations and private companies provide a variety of analytical and investigative tools for penetrating terrorist operations on the Internet. For example, the Washington-based SITE Intelligence Group routinely monitors, translates, and posts information from terrorist Web sites and often shares that information with U.S. intelligence agencies.

Finally, software and hardware providers continue to respond to the needs of the marketplace with new services and products to counter illicit online activity, from combating unauthorized intrusions and countering denial-of-service attacks to preventing the disruption or exploitation of systems or data. Providing security services and products is a multibillion-dollar-a-year industry.

35. InfraGard, "About InfraGard," at *www.infragard.net/about.php?mn=1&sm=1-0* (January 31, 2008).
36. *Ibid.*
37. Eric Swedlund, "UA Effort Sifting Web for Terror-Threat Data," *Arizona Daily Star*, September 24, 2007, at *www.azstarnet.com/allheadlines/202724.php* (January 31, 2008).
38. Marie-Hélène Boccara, "Islamist Websites and Their Hosts Part I: Islamist Terror Organizations," Middle East Media Research Institute *Special Report* No. 31, July 16, 2004, at *http://memri.org/bin/articles.cgi?Page=archives&Area=sr&ID=SR3104* (January 29, 2008), and Marie-Hélène Boccara and Alex Greenberg, "Islamist Websites and Their Hosts Part II: Clerics," Middle East Media Research Institute *Special Report* No. 35, November 11, 2004, at *http://memri.org/bin/articles.cgi?Page=archives&Area=sr&ID=SR3504* (January 29, 2008).
39. U.S. Military Academy, Department of Social Science, Combating Terrorism Center, *The Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda*, March 2006, at *http://ctc.usma.edu/imagery/imagery.asp* (January 29, 2008).

Reinforcing the Cyber Arsenal

A war is raging on the Internet—a contest of action and counteraction between legitimate users and malicious actors that range from state-sponsored hackers to terrorists and transnational criminals. However, the perception that the United States is defenseless in the face of illicit exploitation of computer networks is far from accurate. Both the government and the private sector possess significant capabilities.

Nevertheless, there is little room for complacency. New computer advances create new vulnerabilities. The surety of information systems and the capacity to deter, disrupt, or exploit malicious Internet activity will require developing capabilities proactively and responding in a timely manner to emerging threats.

Washington is struggling "with understanding and harnessing information technologies and the prospects for cyber-warfare, but these challenges may represent merely the dawn of an age in which military competition is defined by commercial research and development and consumer choice."[40] The federal government is a fairly minor customer in the multitrillion-dollar transnational information industry.

The initiatives that will likely best serve the United States and its friends and allies in the cyber conflicts of the 21st century will be those derived from the private-sector experience, coupled with emerging military and intelligence capabilities to conduct information warfare and law enforcement measures to combat cybercrime. What is required is a national framework that builds on these capabilities, encouraging them to collaborate and reinforce one another. They should form the cornerstone of smart strategies for fighting and winning against the cyber threats of the future.

Several principles for cyber security and competition should guide U.S. efforts. Specifically, the U.S. should:

- **Adopt best practices.** Both government agencies, such as the National Institute for Standards and Technology, and the private sector should continue to develop best practices and lessons learned.[41] These can be effective tools. Ensuring that these practices are continuously updated and applied should be government's first priority. Only programs that establish clear tasks, conditions, and standards and that ensure rigorous application will keep up with determined and willful efforts to overcome surety efforts.
- **Employ risk-based approaches.**[42] All information programs should include assessments of criticality, threat, and vulnerability as well as measures to reduce risks efficiently and effectively.
- **Foster teamwork.** Cybersecurity is a national responsibility that requires global cooperation. The United States must maintain effective bilateral and multinational partnerships to combat cyber threats.[43] These efforts should include rigorous measures to prevent the export of sensitive technologies to malicious actors, as well as persistent vigilance to ensure that adversarial states and transnational terrorist and criminal groups do not penetrate U.S. companies that provide essential national capabilities and sensitive national security services.
- **Exploit emergent private-sector capabilities.** Critical capabilities could come from many sources, including small companies and foreign countries.[44] The U.S. government needs to become a more agile consumer of cutting-edge commercial capabilities.
- **Focus on professional development.** Most government information programs underperform

40. James Jay Carafano, "Sustaining Military Capabilities in the 21st Century: Rethinking the Utility of the Principles of War," Heritage Foundation *Lecture* No. 896, September 6, 2005, at *www.heritage.org/Research/NationalSecurity/hl896.cfm*.
41. For example, see Mark A. Sauter and James Jay Carafano, *Homeland Security: A Complete Guide to Understanding, Preventing and Surviving Terrorism* (New York: McGraw-Hill, 2005), pp. 200–202.
42. *Ibid.*, pp. 287–290.
43. James Jay Carafano and Richard Weitz, "Enhancing International Collaboration for Homeland Security," Heritage Foundation *Backgrounder* No. 2078, October 18, 2007, at *www.heritage.org/Research/HomelandDefense/bg2078.cfm*.

because they lack clear requirements, have unrealistic projections of the resources required to implement them, and lack attentive senior leadership. All of these problems can be addressed by maintaining a corps of experienced, dedicated service professionals. National security professionals must have "familiarity with a number of diverse security-related disciplines…and practice in interagency operations, working with different government agencies, the private sector, and international partners."[45] These skills and attributes must include expertise in cyber operations, as well as in developing and managing new systems.

Washington can do better in preparing to respond to current and future cyber threats. Long-term commitment and sound initiatives are needed, not massive reorganization and massive infusions of government cash. These initiatives should push for better and faster acquisition of commercial services; better and smarter management of military, intelligence, and information technology programs; and better and sustained professional development of federal, state, local, and private-sector leaders.

Next Steps

Washington needs to accept that cyberwar will be an enduring feature of the long war on terrorism—perhaps continuing even after the "long war" is won. Thus, Washington should:

- **Fund cyber initiatives for the long term.** In the past, funding and attention from Congress and the Administration have come in "fits and starts." This practice is counterproductive and should be ended. For example, DHS programs should be funded consistently at about $1 billion annually in constant dollars. In particular, Einstein, a system that monitors network gateways for computer viruses and other malicious computer activity, should be fully funded. Additionally, the budgets of the Departments of Defense, Justice, and State and the intelligence community should adequately reflect their cyber missions, including protecting U.S. infrastructure, fighting cybercrime and network intrusions, and combating international espionage, sabotage, and disinformation activities.
- **Implement the Defense Science Board's recommendations for improving the surety of critical software and microchip components.** These recommendations include enhancing education and training for the acquisition community on cyber issues, ensuring robust resources for conducting risk assessments and assurance programs for mission-critical systems, improving the quality and surety of Defense Department software, and conducting advanced research on vulnerability detection and mitigation for software and hardware.
- **Continue to emphasize the information-sharing environment**, as well as various programs under the National Infrastructure Protection Plan that promote effective public–private cooperation on cyber issues.

The Way Forward

There are no silver bullets to ensure that Americans can roam the information superhighway freely and safely in the 21st century. Nor are there any guarantees that malicious actors can be kept on the sidelines. On the other hand, consistent, adequately funded programs should give Americans the confidence that they can outcompete any adversary in the 21st century.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation. Richard Weitz, Ph.D., is Senior Fellow and Director of Program Management at the Hudson Institute.

44. For example, see James Jay Carafano and Paul Rosenzweig, "Protecting Privacy and Providing Security: A Case of Sensible Outsourcing," Heritage Foundation *Backgrounder* No. 1810, November 5, 2004, at *www.heritage.org/Research/HomelandSecurity/bg1810.cfm*.

45. James Jay Carafano, "Missing Pieces in Homeland Security: Interagency Education, Assignments, and Professional Accreditation," Heritage Foundation *Executive Memorandum* No. 1013, October 16, 2006, at *www.heritage.org/Research/HomelandSecurity/em1013.cfm*.