Backgrounder

Published by The Heritage Foundation

No. 2218
December 16, 2008

Building Cyber Security Leadership for the 21st Century

James Jay Carafano, Ph.D., and Eric Sayers

The issue of cyber security, cyber competitiveness, and cyberwarfare has weighed heavily on the minds of policymakers as the severity and complexity of malicious cyber attacks have intensified over the past decade. These attacks, directed against both the public and private sectors, are the product of a heterogeneous network of state and non-state actors whose actions are motivated by a host of factors. Helping to ensure that the federal government achieves a high level of competency on cyber security issues is an imperative for the next Congress.

Indicative of how important cyber security has become, Director of National Intelligence Mike McConnell raised this issue for the first time this past February as part of his testimony on the 2008 Annual Threat Assessment. When asked if he believed the United States was prepared to deal with cyber-security threats to the civilian and military infrastructure, McConnell noted that the country is "not prepared to deal with it. The military is probably the best protected, the federal government is not well protected, and the private sector is not well protected. So the question is: How do we take some of the things that we've developed for the military side, scale them across the federal government? And then the key question will be: How do we interact with the private sector?" Properly answering these questions begins with developing cyber-strategic leadership skills in the U.S. government and private sector.

Even as Washington wrestles with issues concerning organization, authorities, responsibilities, and

Talking Points

- Cyber security, cyber competitiveness, and cyberwarfare have weighed heavily on policymakers as the severity and complexity of cyber attacks have intensified over the past decade.
- Washington must place more emphasis on developing leaders who are competent to engage on cyber issues.
- The U.S. needs leaders who understand the need for strategies of resiliency—methods for ensuring that basic structures of global, national, and local economies remain strong after a cyber attack, other malicious acts, or disasters.
- A cyber-strategic leadership program is necessary for constructing a resiliency strategy for the 21st century. Cyber-strategic leadership is a set of knowledge, skills, and attributes essential to all leaders at all levels of government and the private sector.

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/bg2218.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

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

programs to deal with cyber competition, it must place more emphasis on developing leaders who are competent to engage in these issues. This will require a professional development system that can provide a program of education, assignment, and accreditation to develop a corps of experienced, dedicated service professionals who have an expertise in the breadth of issues related to the cyber environment. This program must be backed by effective public-private partnerships that produce cutting-edge research, development, and capabilities to operate with freedom, safety, and security in the cyber world.

What's at Stake: The Heartbeat of America

Over the past quarter century, the cyberspace domain has rapidly expanded to dominate almost every aspect of human interaction. Americans now depend on cyberspace more then ever to manage their banking transactions, investments, work and personal communication, shopping, travel, utilities, news, and even social networking. Indeed, the global online networks that carry people, goods, information, and services make the world what it is today. With this growing dependence inevitably comes an increased vulnerability. A massive interference with global trade, travel, communications, and access to databases caused by a worldwide Internet crash would create an unprecedented challenge, particularly if it occurred concurrently with any requirement to deploy U.S. forces.[1] Additionally, an attack aimed solely at the U.S., similar in scope to the cyber attacks suffered by Estonia in April and May 2007, could severely disrupt the U.S. economy and increase Americans' concerns regarding their vulnerability.

How to Think About the Problem: It's a Competition

Addressing cyber issues begins with the premise that all national security challenges are a series of actions and counteractions between competitors, and inquiring how these competitions might progress in the future. Looking for single "silver-bullet" solutions will not work. There is no technology, government policy, law, treaty, or program that can stop the acceleration of competition in the cyber universe.

Accepting this premise (that an evolving cyber competition is a permanent character of the global environment) requires responses that offer a comprehensive, multi-disciplinary approach to analysis: looking at the full range of factors that shape and alter the security environment of the future including social, political, technological, and economic trends, as well as dynamic responses that eschew one-time or simple technical fixes to security challenges.

Required—Strategies of Resiliency

Strategies must be national in character and international in scope. Nearly every domestic cyber program—from managing movement of goods, people, services, and ideas to controlling a border to investigating terrorist groups—requires international cooperation. This dimension of safeguarding the home front is nowhere more important than in addressing national infrastructure, supply-chain issues, and public-private partnerships. America is part of a global marketplace with a global industrial base. Virtually no nation is self-sufficient.[2]

Efforts to safeguard the homeland tend to focus solely on the unrealistic task of protecting infrastructure. However, the politically charged "failure is not an option" approach to classify all infrastructure as "critical" is detrimental to prioritizing national security missions.

Instead, the U.S. needs leaders who understand the need for creating and implementing strategies of resiliency, or methods for ensuring that basic structures and systems of global, national, and local economies remain strong even after a cyber attack or other malicious acts or acts of war.[3]

[1] See, for example, Madeline Drexler, *Secret Agents: The Menace of Emerging Infections* (Washington, D.C.: John Henry Press, 2001), pp. 158–200.

[2] See, for example, James Jay Carafano and Richard Weitz, "Enhancing International Collaboration for Homeland Security and Counterterrorism," Heritage Foundation *Backgrounder* No. 2078, October 18, 2007, at *http://www.heritage.org/Research/HomelandDefense/bg2078.cfm*.

A strategy of resiliency does not mean abandonment of preventive measures. At its core, resiliency is far more complex—and effective—than simply protecting critical infrastructure against natural and man-made threats. Protection alone cedes the initiative to the enemy.

Required: Cyber-Strategic Leaders

Due to the vulnerability of cyberspace, one initiative that should be prominent in constructing a resiliency strategy for the 21st century is a cyber-strategic leadership program. Cyber-strategic leadership is not a specific technical skill or person, but a set of knowledge, skills, and attributes essential to all leaders at all levels of government and in the private sector.

The recipe of education, assignment, and accreditation that worked so successfully following the Goldwater–Nichols Act of 1986 can also be used to foster critical interagency skills among national security professionals. No institutions are currently designed in Washington, academia, or elsewhere to carry out such a task. A national effort with national standards should be initiated along with a new government institution to help foster interagency learning should be built in Washington, D.C. This professional development program could integrate a shared body of common knowledge, practices, and experiences, as well as trust and confidence among practitioners. Amongst the skills and attributes this institution could provide would be an expertise in the cyber environment, risk management, best practices, effective interagency cooperation, and public-private partnerships. Just as senior leaders in government and the private sector are expected to have an understanding of accounting and informational technology (IT), a working knowledge of cyber security must also become commonplace.

Knowledge, Skills, and Attributes for Cyber-Strategic Leaders

Understand the Cyber Environment. Beginning in 1988 with the infamous "Morris Worm" attack, cyber security has grown in importance along with the degree of reliability the United States and other nations have placed on the cyber domain.

The effectiveness of cyberwarfare stems from its dynamic characteristics. In addition to low costs to entry, making it more attractive to terrorists and other non-state actors inclined to pursue low-end asymmetric strategies, the historical boundaries of warfare do not apply to the cyber realm.

Although decentralized, cyberspace remains dependent on the physical network of computer servers, fiber-optic cables, and the immense system of cables that have been laid across the world's oceans. A familiarity with the physical aspects of cyberspace forms the foundation of a larger education on the topic.

The complexities of cyberspace begin with the distinction between its two existing theaters. First, the commercial Internet. Reserved for the day-to-day activities of the public, and traditionally the target of non-state actors, the vulnerability of this theater has been magnified in the wake of the Estonia and Georgia cyber attacks that occurred in April and May 2007 and August 2008, respectively. Second, the military network. Over the past two decades, as the military has attempted to enhance its warfighting capabilities through network-centric warfare, an increased reliability on information technology has had the cumulative effect of ensuring a growing liability should the network fall under attack.[4]

There are various types of actors that may pose a threat to the commercial and military cyber networks. First, individuals acting on their own to exploit security gaps or commit cyber crimes, such as identify theft. These hackers are commonly referred to as "Black Hats." Second, cyber terrorists attempting to manipulate the cyber environment to advance political or social objectives.[5] Islamist hackers took their fight to the target-rich environment of the Internet years ago. Thanks to its low barriers to entry, the cyber environment has proven itself to be one of the most efficient asymmetric

[3] James Jay Carafano, "Resiliency and Public-Private Partnerships to Enhance Homeland Security," Heritage Foundation *Backgrounder* No. 2150, June 24, 2008, at *http://www.heritage.org/Research/HomelandDefense/bg2150.cfm*.

[4] Rebecca Grant, "Victory in Cyberspace," The Air Force Association, October 2007, at *http://www.afa.org/media/reports/victorycyberspace.pdf* (December 2, 2008).

tools for Islamist terrorists to incite hatred, violence, and plan and carry out attacks.

Finally, nation-states are increasingly employing cyberwarfare to attack other states or entities, either solely in the cyber domain or as part of a full-spectrum military maneuver.[6] Specifically, states like China and Russia, which remain inferior to the United States militarily, have identified America's cyberspace vulnerability and worked diligently to exploit it.[7] As we have learned from Chinese military journals, the People's Liberation Army (PLA) has focused intensely on attacking the U.S. military's C4ISR network with a variety of weapons, including anti-satellite (ASAT) weapons and cyberwarfare.[8]

The predominant tool used for cyber attacks are botnets. A botnet is a network of computers that have been compromised by malicious code and may be remotely controlled by a single computer, called a "bot herder" or "bot master." When the power of thousands of computers is combined, it can be used to launch denial-of-service attacks to shut down desired Web sites. Due to the rapidly changing nature of software, including improved commercially available security programs, the dissemination of botnet code has evolved from using e-mail attachments to pop-up spam messages and even silent uploads that take advantage of vulnerabilities in Internet browsers.[9]

Cyber espionage constitutes another threat. Not only are such tactics being used to advance the interest of private corporations as they work to compete in the global market, but states have also employed this tool to both monitor the capabilities of adversaries and steal valuable, top secret, and proprietary information. Everything from the Pentagon's most sensitive plans to invaluable intellectual property is at risk. Many officials have identified China as the main culprit in this effort, citing numerous major attacks against the Department of Defense and defense contractors that originated from the Chinese mainland.[10]

Finally, international legal mechanisms that govern cyber activity remain wanting. This is due in part to the decentralized nature of cyber attacks. During the Estonia attacks, for instance, although the perpetrator was believed to be the Russian government, and many computers that assisted in the attack were located in Russia, computers all over the world were used to launch the attack. Any direct evidence linking the attacks to Russia was thus highly circumstantial. During the crisis, questions lingered regarding what magnitude of cyber attack or evidence of perpetrators was necessary to invoke an Article V response under the auspices of NATO. Additionally, questions were asked regarding what constituted an appropriate response from Estonia and other NATO members. NATO Secretary General Jaap de Hoop Scheffer largely summarized the prevailing answers to these questions when he stated that "no member state is protected from cyber attacks."[11] Efforts to construct a framework to help guide the activities of varying actors in cyberspace remain essential.

[5] James Jay Carafano and Richard Weitz, "Combating Enemies Online: State-Sponsored and Terrorist Use of the Internet," Heritage Foundation *Backgrounder* No. 2105, February 8, 2008, pp. 3–4, at *http://www.heritage.org/Research/nationalSecurity/bg2105.cfm*.

[6] *Ibid.*, pp. 1–3.

[7] See John J. Tkacik, Jr., "Trojan Dragons: China's International Cyber Warriors," Heritage Foundation *WebMemo* No. 1735, December 12, 2007, at *http://www.heritage.org/research/asiaandthepacific/wm1735.cfm*, and James Jay Carafano, "When Electrons Attack: Cyber-Strikes on Georgia a Wake-Up Call for Congress," Heritage Foundation *WebMemo* No. 2022, August 13, 2008, at *http://www.heritage.org/research/nationalsecurity/wm2022.cfm*.

[8] Roger Cliff, Mark Burles, Michael S. Chase, Derek Eaton, and Kevin L. Pollpeter, "Entering the Dragon's Lair: Chinese Antiaccess Strategies and Their Implications for the United States," RAND Corporation, 2007, p. 18, at *http://www.rand.org/pubs/monographs/2007/RAND_MG524.pdf* (December 2, 2008).

[9] Clay Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," Congressional Research Service, January 29, 2008, at *http://www.fas.org/sgp/crs/terror/RL32114.pdf* (December 2, 2008).

[10] Josh Rogin, "Cyber Officials: Chinese Hackers Attack 'Anything and Everything,'" FCW.com, February 13, 2007, at *http://www.fcw.com/online/news/97658-1.html* (December 4, 2008).

Think Strategically. There are many "first order" questions that deserve serious thought as the nation considers the next steps in keeping the "cyber commons" open to the free flow of services and ideas while thwarting the activities of malicious actors. These include everything from defining how "deterrence" works in cyberspace to understanding the realistic application of the "rule of law" in a place that in many ways is still lawless. Strategic thinkers must understand the costs and benefits of operating in cyberspace, the nature of the actors, the character of the environment, and how traditional concepts of security and war and peace translate to the cyber world.

Understand Risk and Risk Management. Quantifying and determining optimal responses to risk is a process called risk management. Properly assessing and reducing risk is central to a resiliency strategy. There are three types of risk assessment methodologies, all consisting of similar components.[12]

- **Threat assessment**: Examines what an adversary can accomplish and with what degree of lethality or effect.
- **Criticality assessment:** Evaluates the effect that will be achieved if the adversary accomplishes his goals. This examines both physical consequences, social and economic disruption, and psychological effects. Not all consequences can be prevented. In order to assist in prioritization, there is a process designed to identify the criticality of various assets: What is the asset's function or mission and how significant is it?
- **Vulnerability assessment:** Studies a country's vulnerabilities and how they can be mitigated, including weaknesses in structures (both physical and cyber) and other systems and processes that could be exploited by terrorists. It then asks what options are available to reduce the vulnerabilities identified or, if feasible, to eliminate them.

Adapt Best Practices. Best practices and lessons learned can be effective tools. Ensuring that these are updated and applied should be government's first priority. Only programs that establish clear tasks, conditions, and standards and ensure that they are rigorously applied will keep pace with determined and willful efforts to overcome security efforts. This is especially true in the cyber domain, where the center of gravity is persistently shifting as the rapid evolution of technology and skills pull it in new directions.

Understand Effective Interagency and Public-Private Cooperation. Properly understanding the performance of the interagency process requires dividing it into three components.

- **Policy:** The highest level of the interagency process. At this level, policymakers make broad agreements about how they will support overall U.S. policy. Improvements in this area require a renewed focus on the qualities and competencies of executive leadership, and an intelligence capability and information-sharing culture that allows leaders to obtain the highest-quality information available so that they are positioned to make the best-informed decisions.
- **Operations:** It is at this level where the record of government is mixed. While the Department of Defense's Combatant Command structure has proven itself capable of managing military operations at the regional level, there are very few other established bodies that are able to monitor and manage operations over a geographical area.
- **Field activities:** Interagency cooperation on the ground has generally been effective. The country teams led by U.S. ambassadors around the world offer a strong example. However, when challenges grow beyond the control of the local government apparatus, robust support mechanisms are normally lacking. Attention to improved doctrine (how to best conduct joint planning and

[11] Tony Halpin, "Putin Accused of Launching Cyber War," May 18, 2007, *Times Online*, at *http://www.timesonline.co.uk/tol/news/world/europe/article1805636.ece* (December 2, 2008).

[12] James Jay Carafano, "Risk and Resiliency: Developing the Right Homeland Security Public Policies for the Post-Bush Era," testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, United States House of Representatives, June 24, 2008, at *http://www.heritage.org/Research/HomelandSecurity/tst062408a.cfm*.

> response during a cyber crisis), sufficient investment in human capital, and appropriate decision making are required in such situations. Effective interagency cooperation does not begin at the policy level, but requires a more responsive operational environment that can meet the challenges of local leadership.[13]

While it is the responsibility of government to prevent terrorist attacks, determining the criticality of assets should be a shared public-private activity. This starts by establishing a common appreciation of roles and responsibilities for the public-private partnership.

Because vulnerability should be the primary responsibility of the partner that owns, manages, and uses the infrastructure, it is largely the private sector's duty to address vulnerability by taking reasonable precautions in much the same way that society expects the private sector to take reasonable measures for safety and environmental protection.[14]

An Agenda for the New Administration

Step 1: Facilitate Cross-Talk. There is a plethora of ongoing cyber security and cyberwarfare initiatives. The tendency of any new Administration is to conduct grand reviews of existing efforts, issue sweeping strategies, centralize management, and reorganize operations and responsibilities. That is a mistake. Such moves are as likely to stunt momentum and slow innovation as they are to achieve any efficiencies of operation. Instead, the Obama Administration's first priority must be to facilitate cross-talk between the members of the national "cyber team."

Today, those responsible for "offensive" cybersecurity measures (for example, identifying and countering malicious actors) have little contact, familiarity, or collaboration with those working on "defensive" measures, and vice versa. Likewise, agencies and organizations conducting "covert" activities have scant interaction with those engaged in "public" programs. This must change. To close gaps, minimize duplication and overlap, facilitate joint action, and build trust and confidence between members of the public-private team, establishing routine and consistent dialogue must be an immediate priority. This is a vital first step in building a community of professional cyber-strategic leaders.

Step 2: Research, Research, Research. Building cyber-strategic leaders will be like building castles on sand unless the knowledge and skills imparted to them is based on comprehensive, practical, and unbiased research. As a 2007 Computer Science and Telecommunications Board research report concluded, however, the national research and development program is wholly inadequate:

> [B]oth traditional and unorthodox approaches will be necessary. Traditional research is problem-specific, and there are many cybersecurity problems for which good solutions are not known.… Research is and will be needed to address these problems. But problem-by-problem solutions, or even problem-class by problem-class solutions, are highly unlikely to be sufficient to close the gap by themselves. Unorthodox, clean-slate approaches will also be needed to deal with what might be called a structural problem in cybersecurity research now, and these approaches will entail the development of new ideas and new points of view that revisit the basic foundations and implicit assumptions of security research. Addressing both of these reasons for the lack of security in cyberspace is important, but it is the second—closing the knowledge gap—that is the primary goal of cybersecurity research…"[15]

The report goes on to lay out an appropriate research agenda including such issues as deterring would-be attackers and managing the degradation

[13] James Jay Carafano, "Managing Mayhem: The Future of Interagency," March 1, 2008, at *http://www.heritage.org/press/commentary/ed030308b.cfm*.

[14] Carafano, "Resiliency and Public-Private Partnerships to Enhance Homeland Security."

[15] Computer Science and Telecommunications Board, *Toward A Safer and More Secure Cyberspace* (Washington, DC: National Academies Press, 2007), p. 61.

and reconstitution of systems in the face of concerted attacks.

Step 3: Get Safe. Encouraging innovation is perhaps the quickest and most effective way to promote public-private engagement and build a national ability to mitigate and respond to cyber threats. Providing liability protection is one proven means of promoting private-sector innovation.

Since 9/11, Congress has acted decisively and to good effect in one area of liability protection: The Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act lowered the liability risks of manufacturers that provide products and services used in combating terrorism. The act, passed in 2002, protects the incentive to produce products that the Secretary of Homeland Security designates as "Qualified Anti-Terrorism Technologies." The Department of Homeland Security has made a concerted effort to implement the program, and about 200 companies have obtained SAFETY Act certification.[16] This program should be used to accelerate the fielding of commercial products and services for cyber security.

Step 4: Implement the National Security Professional Development Program. The Obama Administration should build on the National Security Professional Development, a process to educate, certify, and track national security professionals.[17] This program should be modified based on the experience of the last two years in attempting to implement the program and be used to develop leaders skilled in cyber-strategic leadership and other critical national security missions.[18]

The First Step on a Long Road

Efforts to use the cyber domain for malicious purposes have matured in scope and sophistication over the past two decades. This threat will only intensify as terrorists continue to embrace its low costs to entry and states operationalize its power as a new domain of 21st-century warfare. Meeting this challenge in both the public and private sectors will require careful planning and consideration in the coming years. Initiating a professional-development, cyber-strategic leadership program to begin training future leaders in the complexities of the cyberspace arena is imperative to the future security of America's cyber infrastructure.

—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, a division of the Davis Institute, at The Heritage Foundation. Eric Sayers is a Research Assistant in the Allison Center.

[16] James Jay Carafano, "Fighting Terrorism, Addressing Liability: A Global Proposal," Heritage Foundation *Backgrounder* No. 2138, May 21, 2008, at *http://www.heritage.org/Research/NationalSecurity/bg2138.cfm*.

[17] The White House, "Executive Order: National Security Professional Development," May 2007, at *http://www.whitehouse.gov/news/releases/2007/05/20070517-6.html* (December 2, 2008).

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