America at Risk
Memo

**Protect America Month: Providing for the Common Defense in the 21st Century**

The Heritage Foundation's Protect America Month is a month-long campaign focusing on the need for increased defense spending in the 21st century. America still faces serious threats in the world and now is not the time to weaken our military through defense budget cuts.

No. AR 11-03 • May 16, 2011

# Time for America to Get Cyber-Serious

*Paul Rosenzweig and James Jay Carafano, Ph.D.*

The online threats facing America read like an ever-expanding encyclopedia of dangers to the freedoms, prosperity, and security of all Americans. Cybersecurity has become a crucial component of national security. Responses to cyber threats, however, have largely lagged because of a focus on technologies rather than the people behind the technologies.

Cyber competition is just one instrument that America's enemies are using to undermine the common defense. To meet these challenges, the United States and its allies need to get cyber-serious.

## There Be "Real" Dragons

The Web is a target-rich environment. The Department of Defense (DOD) alone has 3.5 million computers and 35 internal networks in 65 countries, many of which depend on commercial systems. According to the Defense Science Board, not only do cyber attacks represent a general threat, but military and DOD operations are, to a significant extent, susceptible to their effects.[1]

Government and private information networks are increasingly under attack. According to a 2001 report from the General Accounting Office (now known as the Government Accountability Office):

> Daily, DOD identifies and records thousands of "cyber events," some of which are determined to be attacks against systems and networks. These attacks may be perpetrated by individuals inside or outside the organization, including hackers, foreign-sponsored entities, employees, former employees, and contractors or other service providers.[2]

Enemies online fall into several categories. State actors come in three stripes: aggressors, enablers, and slackers. Foremost among the ranks of *aggressor states* is China. China's record of cyber-espionage is legion. It is estimated that half of the world's intellectual capital is in the United States. Most of it is online. Chinese nationals are trying to steal it.

*Enabler states* are ones that consciously seek ill for another country but only indirectly allow or actively promote malicious online activity. Russia is a classic enabler that has done little to stem the tidal wave of illicit cyber activity within its borders, much of it aimed at the United States.

*Slacker states* are nations with lax laws or means of enforcement, which makes them powerless to prevent other state or non-state groups from exploiting their territory for malicious activity. Pakistan, nominally a U.S. ally in the global war against terrorists, is a classic slacker state when it comes to cyber competition. Pakistan is one of the fastest growing base camps for malicious online activity from both Islamist extremist groups and criminal activity.

Non-state actors are trouble online as well. Transnational cyber criminal activity is exploding, much of it through software designed to steal password and financial and personal identification information. Internet security services identified 1,656,227 new malicious codes in 2008—a 265 percent increase over the previous year.

Non-state cyber threats include Islamist hackers who have promoted the tactic of "electronic jihad," attacking "enemy" Web sites to undermine morale and harm

The Heritage Foundation
LEADERSHIP FOR AMERICA

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.

economic and military infrastructure. Many Islamist Web sites host forums that discuss how to conduct such Web-based attacks. Terrorist groups also use the Web for recruiting, fundraising, propaganda, intelligence gathering, and planning operations.

Among the disturbing emergent concerns is that enemies could create a catastrophic failure in Supervisory Control and Data Acquisition (SCADA) systems, which monitor and control most U.S. infrastructure. Such an attack could cause power outages, spark explosions, and unleash fuel spills. Although these systems are not part of the Internet, governments and the private sector have been employing "enterprise-wide" architectures that link SCADA systems to the Web. As a result, they have potentially created a large number of gateways into some of America's most sensitive networks. The recent Stuxnet computer worm is highly sophisticated malware designed to target SCADA systems.

## Guarding the Frontier

Treating national security cyber competition as just a "computer problem" is a mistake. For every firewall or virus protection fielded, malicious actors will invent new ways to circumvent them. The U.S. needs to be prepared to deal with all aspects of the pursuit of cyber actors, including legal, financial, diplomatic, propaganda, covert operations, and other means of finding the enemy's weakest link and exploiting it.

The effort to make America a solid cyber competitor rests on three pillars.

1. **Strong allies.** Cyberspace is not an ungovernable Wild West. Nations can act within their sovereign cyberspace, where infrastructure is inside their borders. The U.S. should work in concert with like-minded nations committed to freedom, prosperity, and security to combat bad actors in cyberspace. Cybersecurity is also becoming an increasingly important issue for NATO. The U.S. should be building strong partnerships with nations like India as well.
2. **Strong cyber leaders.** The age in which cyber issues were the chief information officer's problem—in either government or the private sector—is over. Leaders in government and the private sector should develop the skills, knowledge, and attributes of cybersecurity leadership. They need the education, training, and experience that qualify them to be real cyber leaders.
3. **Strong cyber citizens.** Most malicious online activity occurs so effortlessly because of poor individual security practices. Many fall victim to the most clumsy "social engineering" ruses used to steal passwords or inject viruses into computer networks, such as clicking on a link that says, "You have to see this." Individual cyber-preparedness is the civil defense of the 21st century.

## A Very Real Threat

There is a role for all Americans in defeating bad cyber actors online. But the most important thing that public officials, business leaders, and private citizens should do is recognize the scope of the cyber threat and the nation's current vulnerabilities.

*—**Paul Rosenzweig** is the Principal at Red Branch Consulting, PLLC, and a Visiting Fellow at The Heritage Foundation. He is a former Deputy Assistant Secretary for Policy at the Department of Homeland Security. **James Jay Carafano, Ph.D.**, is Deputy Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Director of the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Davis Institute, at The Heritage Foundation.*

[1] Defense Science Board, *Capability Surprise, Volume I: Main Report*, U.S. Department of Defense, September 2009, at *http://www.acq.osd.mil/dsb/reports/ADA506396.pdf* (May 11, 2011).

[2] U.S. General Accounting Office, *Information Security: Challenges to Improving DOD's Incident Response Capabilities*, GAO–01–341, March 2001, p. 4, at *http://www.gao.gov/new.items/d01341.pdf* (May 11, 2011).

This paper, in its entirety, can be found at:
***http://report.heritage.org/ar1103***