HOMELAND SECURITY 2020

The Future of Defending the Homeland

How can we ensure that we can take on the evolving nature of future threats?

This is part of a series of Heritage publications dedicated to devising the right security policy agenda for the next decade.

No. 4 • August 26, 2010

Cyber Security: A Complex "Web" of Problems

Paul Rosenzweig

The Obama Administration made a strong start at rationalizing U.S. cyber security policies, including an initial 100-day review of existing protocol and the creation of a "cyber coordinator" position.[1] Unfortunately, the momentum with which the Administration started seems to have waned. As a result, though the U.S. is better organized now than it was three years ago, much work remains to be done on the complex problems that involve cyber security.

Today, as it pertains to cyber security, America still needs clearer lines of authority within the federal government and a more coherent structure of public–private interaction to allow for effective action. That structure should provide for greater and more effective control and coordination of the federal effort. Though current cyber coordinator Howard Schmidt has begun well, he should become a cyber leader with more directive authority.

A Growing Need

The need for greater coordination and control is not simply idle speculation. Consider the following example: A few years ago, the Central Intelligence Agency (CIA), working cooperatively with Saudi Arabia, set up a "honey pot" Web site to attract jihadi sympathizers. By all reports the site served as a useful intelligence-gathering tool, giving the unseen CIA and Saudi observers insights into the activities and interests of the terrorists who frequented the site.

By 2008, however, it had become apparent that some terror groups were using the site to infiltrate jihadists into Iraq, where these fighters would join the insurgency, potentially threatening the lives of American troops. The National Security Council convened a group of representatives from the Department of Defense (DoD), CIA, Department of Justice, the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) to consider the matter. Eventually, over the CIA's objections, a DoD team from Joint Functional Component Command–Network Warfare "took down" the site. Their actions caused collateral effects as far away as Germany and disappointed America's Saudi collaborators.

This event shows just how confused America's cyber policies are. Think of it—one American team from DoD actually attacked and destroyed a Web site that another agency of government, the CIA, had created and was using. That reflects a real lack of coordination at the top and a real dearth of clear policy direction for those operating in the field.

A more systematic example of the disconnect within the federal government occurred in October 2009, when the NSA announced that it was breaking ground on a new facility in Utah to provide DHS with "intelligence and warnings related to cyber security threats, cyber security support to defense and civilian agency networks, and technical assistance."

In November 2009, DHS opened its own new facility, the National Cybersecurity and Communications Integration Center in Arlington, Virginia. This facility will "house the National Cyber Security Center, which coordinates cyber

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 2009, at *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf* (August 24, 2010).

The Heritage Foundation
LEADERSHIP FOR AMERICA

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

security operations across government, the National Coordinating Center for Telecommunications, which operates the government's telecommunications network, and the United States Computer Emergency Readiness Team, which works with industry and government to protect networks and alert them of malicious activity."[2] The two new facilities are, at least facially, somewhat duplicative, indicating a continuing need for strategic level cyber coordination.

Unfocused Cyber Strategy

Duplicative effort and the waste it entails are not the only risks posed by uncoordinated federal activity. More significantly, the lack of coordination reflects an inability to bridge a cultural gap between the openness of the Silicon Valley and the secrecy of a national security environment. As Rod Beckstrom (former director of the DHS National Cybersecurity Center) noted, which agency leads the cyber security effort makes a difference because an "intelligence culture is very different from network operations or security culture."

In the absence of leadership and control from the top, it looks like the NSA is forging ahead in efforts to protect the cyber domain. For example, despite DHS's statutory authority and responsibility for protecting civilian infrastructure, it appears that it is NSA (and not DHS) that has begun a program called "Perfect Citizen" to detect cyber assaults on private infrastructure.[3] Though details of this new program are hazy,[4] it appears possible that the program will conflict with, or at least duplicate, programs operated by DHS. It may also presage an effort by NSA to exert more control over civilian networks generally.

At present, the White House cyber coordinator lacks the authority to de-conflict these competing structures. His role apparently lacks any authority over operational decisions or budgetary priorities. The result, beyond the perception of conflict, is (as a recent Government Accountability Office audit makes clear) continued confusion and overlap of responsibilities.[5]

The dry language of the GAO masks a traditional Washington concern—a battle over turf and budgets—and makes clear that more effort is required. The outcome of this battle matters profoundly.

In short, if this logjam is to be broken, the new cyber coordinator must, in effect, take more direct control. This will require a strong commitment from the White House and a significant increase in the power of the cyber coordinator. It will be necessary to give the coordinator authority to do the following:

- Create a unified cyber security budget account within the President's annual budget submission and work with the NSC to set budget priorities with that account;
- Lead and coordinate the development of cyber security policy (including through chairmanship of a dedicated policy planning group that needs to be chartered);
- Direct agency action in conformance with the budgetary and policy priorities set;
- Have dotted-line authority over and a role in the selection of cabinet-level and sub-cabinet cyber leaders (e.g., the commander of Cyber Command and the head of U.S.-CERT); and
- Develop an enhanced set of objectives derived from the Comprehensive National Cybersecurity Initiative that will contain a set of measurable performance goals and objectives for cyber defense and resilience.

Such authority is essential to the cyber coordinator position.

An Essential Task

The task is assuredly a difficult one. Recent attempts to provide for more centralized authority and control (such as the formation of DHS and the creation of the ODNI) have been only partially successful. But the difficulty of the task does not mean that the effort should not be undertaken—indeed, if it is not, America can only anticipate more self-inflicted wounds of the sort experienced on the Saudi Web site.

—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. This paper is based on work done for the National Academy of Sciences to be included in a forthcoming volume on cyber deterrence.[6]

2. J. Nicholas Hoover, "NSA to Build $1.5 Billion Cybersecurity Data Center," *InformationWeek*, October 29, 2009, at *http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221100260* (August 24, 2010).
3. Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies," *The Wall Street Journal*, July 8, 2010, at *http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704545004575352983850463108.html* (August 24, 2010).
4. J. Nicholas Hoover, "NSA Launches Infrastructure Cybersecurity Program," *InformationWeek*, July 9, 2010, at *http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225702741&cid=RSSfeed* (August 24, 2010).
5. U.S. Government Accountability Office, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO–10–338, March 2010, p. 13.
6. See Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence" (draft July 2010), at (August 24, 2010).

This paper is posted online as Heritage Foundation *WebMemo* No. 2991 and available at *http://report.heritage.org/wm2991.*