WebMemo
Published by The Heritage Foundation
No. 2813
February 23, 2010

The Cybersecurity Enhancement Act of 2009: A Start, But Not Nearly Enough

Paul Rosenzweig and Jena Baker McNeill

On February 4, before several snow storms shut down much of Washington, D.C., the U.S. House of Representatives passed its first cyber security bill of this session. This bill, the Cybersecurity Enhancement Act of 2009, would fund grants and fellowships for cyber research and establish minimum requirements for the National Institute of Standards and Technology (NIST) for government computer networks, among other provisions. While the bill would, if adopted by the U.S. Senate, make some progress toward improving the protection of America's critical infrastructure, the bill makes no hard choices and breaks no new ground in terms of cyber security.

Going forward, the Obama Administration, working with Congress, should lay the foundation for an a renewed focus on cyber security, one centered on the principles of smart security, economic prosperity, robust protection of privacy and civil liberties, and the need for limited government. Good first steps toward this goal would be to improve the quality of oversight and interagency coordination within Congress and the executive branch on cyber issues while updating laws, policies, and doctrines to reflect cyber realities.

The Cybersecurity Enhancement Act of 2009. The bill:

- Calls for a cyber security strategic research and development plan;
- Directs the National Science Foundation (NSF) to create fellowships and give grants for cyber-related research; and
- Requires the NIST to develop checklists and technical standards for cyber security matters.

All of these steps are positive, especially allowing NSF and NIST to spend money (appropriated wisely) on the most valuable and promising research. But research is only one component—and a relatively small one—of a sound national cyberspace doctrine.

For its part, the Obama Administration has tried to make the case for a more extensive approach to cyber security. Yet the White House has failed to robustly address cyber security, while congressional efforts remain scattered and unorganized. Given America's extensive reliance on cyber networks, such an undertaking is important and should be done in a thoughtful and deliberate manner built on these important principles:

- *Economic prosperity.* The private sector conducts its business primarily through cyber networks. Therefore, any legislation that attempts to regulate the cyber realm must take into account the economic interests at stake. Where the federal government does have a legitimate need to regulate, it should do so in a flexible and cost-effective manner.

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandSecurity/wm2813.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy 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.

- *Robust protection of privacy and civil liberties.* If they are to be effective, new cyber doctrines and policies are likely to involve the government in significant new activities on the Internet. That will be a change, and many Americans will rightly be concerned. They will want assurances that even as America acts to stop cyber threats, citizens' fundamental privacy and civil liberties will be protected—and the government should provide these assurances.
- *Limited government.* Undoubtedly, the federal government's responsibility to provide for the common defense extends to the cyber realm. However, the federal government should act only where absolutely necessary—leaving the cyber domain in the hands of private citizens while providing necessary security.

A New Cyber Agenda. Developing an organized framework based on these principles may well require a new paradigm in order to be successful. Currently, the U.S. approaches cyber security through the prism of a security paradigm, with "firewalls" fighting off "distributed attacks" from "botnets." This may be the right concept, but it might not.

The private sector company IBM, for example, has suggested a model for cyber security based on the public health approach. The public health model does not expect to eradicate all illnesses and viruses; rather, it aims to develop immunities, track disease vectors, and work to prevent epidemics. This approach, which could be used to educate the public on how better to prevent cyber "illnesses" before they become a large problem, should be explored under a cyber effort.

Regardless of which model is chosen, there are a few key steps that should be taken before Congress and the Administration can truly begin the process of developing a strong approach to cyber security, including:

- *Create effective oversight mechanisms.* Currently, cyber security is subject to multiple layers of oversight by congressional committees. Often this duplicative oversight has led to conflicting priorities and messages, which in turn impede the creation of a robust cyber effort. Congress should look to streamline oversight of homeland security, including the cyber realm. Furthermore, the Obama Administration should activate the Privacy and Civil Liberties Oversight Board, which has stood empty since August 2007.
- *Organize the interagency.* The Bush Administration did not make much headway organizing and coordinating the federal response to the cyber threat, and the Obama Administration is faring no better. For example, it took the Obama Administration seven months to name a cyber czar—one who would ultimately not have nearly enough authority. The National Security Agency and the Department of Homeland Security remain, apparently, locked in a battle over who will lead the cyber security effort. Meanwhile, the Department of Defense's decision to set up a unified cyber command has yet to become a reality—and its relationship to the civilian sector has yet to be defined. These are challenges that must be sorted through top-level leadership from the White House.
- *Increase coordination with the private sector.* Virtually all of the critical cyber networks are owned and operated by private sector entities, run private sector code, and/or use private sector–manufactured routers and hardware. Most of the non-classified government and military traffic travels on private networks. Today, however, the government's cyber response coordination with the private sector is less than ideal. For security reasons, the government shares limited information with the private sector. Conversely, business incentives often limit the willingness of the private sector to share threat information with each other or with the government. Improving coordination between the existing critical infrastructure sector coordination councils is essential.
- *Update law and policy.* Most cyber-related laws and policies are several years old. Some, like the Privacy Act, which was passed in 1974, are so old that they might as well have been passed in medieval times—at least as far as computer and Internet technology are concerned. Some of the criminal, civil, and national security laws reflect assumptions about Internet architecture

or the attributes of data that are no longer accurate descriptions of how cyber threats actually occur. The U.S. needs to update basic rules and authorities that govern this nation's response to cyber threats.

- *Revise military doctrine.* Many cyber threats are from private actors—hackers or criminals. But some of the most sophisticated threats come from peer-state competitors like China and Russia or non-state terrorist actors. Classic military doctrines on the use of armed forces, deterrence, and proportionality are all based on a conception of kinetic warfare between nation-states. None of these doctrines are easily translated into the cyber realm. Consequently, the U.S. should look to re-conceptualize military doctrines for the new cyber reality.

Need to Do More. The Cybersecurity Enhancement Act of 2009 provides research and education dollars, which can be used to spark innovation in the cyber security realm—a much-needed step toward solving the problems of cyber vulnerability. However, Congress and the Administration still need to do more.

—Paul Rosenzweig is the founder of Red Branch Consulting PLLC. Jena Baker McNeill is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.