WebMemo
Published by The Heritage Foundation
No. 2962
July 16, 2010

Congress Starts Thinking Seriously About Cybersecurity—but More Thinking Needed

Paul Rosenzweig and James Jay Carafano, Ph.D.

Recently, Senators Joseph Lieberman (I–CT), Susan Collins (R–ME), and Thomas Carper (D–DE) introduced the Protecting Cyberspace as a National Asset Act of 2010. This tri-partisan group is the second to offer a cyber solution, the first being a bill introduced by Senators Jay Rockefeller (D–WV) and Olympia Snowe (R–ME), aptly named the Rockefeller–Snowe Cybersecurity Act.

Given the need to develop a cohesive strategy for tackling the security challenges posed by the cyber domain, it is essential that Congress digs into the difficult issues and finds smart solutions—drafting the two bills mentioned above is an important first step. But even more work is required from Congress if America's cybersecurity challenges are to be successfully met. Specifically:

- The U.S. needs a legislative initiative that gets all the pieces exactly right, one which ensures that civil liberties, privacy, and economic prosperity are maintained while securing America's digital infrastructure; and
- Congress needs to pay far greater attention to oversight of the federal enterprise and ensure that the government is investing in human capital—a key component of effective cyber strategic leadership.

A Tale of Two Bills. The Lieberman–Collins–Carper bill's most notable provisions would set performance standards for the protection of information infrastructure. These standards would define the security results desired without telling private industry how to achieve those results. Thus, the bill would direct the Department of Homeland Security (DHS) to create a new office—the National Center for Cybersecurity and Communications—that would work in coordination with the private sector to identify cyber vulnerabilities in critical information infrastructures.

DHS would then consult with Congress and private industry and issue regulations creating risk-based security performance requirements. Those who owned the information infrastructure would be allowed to implement any security measures that DHS agrees would satisfy the security performance requirements.

These owners would have to certify their compliance and be subject to audits, but ultimately the private sector would bear the principal responsibility for figuring out how to secure their infrastructure. Their reward for allowing the government to direct their efforts would be substantial: They would get liability protection, including immunity from punitive damages and limits on non-economic damages.

The bill would also require information infrastructure companies to report "any incident affecting [their] information infrastructure…to the extent the incident might indicate an actual or potential

This paper, in its entirety, can be found at:
http://report.heritage.org/wm2962

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

cyber vulnerability, or exploitation of a cyber vulnerability." The government would serve as a central repository of information about cyber vulnerabilities, enabling it to lead any response. In the past, the private sector has been highly reluctant to provide this sort of information to the government—nobody likes to announce that they have security flaws or to identify exactly where those flaws are. To deal with that problem, the bill prohibits public disclosure of information shared with DHS.

While the Lieberman bill would entrust cybersecurity powers to both a confirmed White House official and a new cybersecurity center at DHS, the Rockefeller–Snowe bill would create a new White House post and require the Department of Commerce to create a scorecard and cybersecurity standards. Building on that proposal, the bill would also require cybersecurity officials to be certified to work on federal networks and critical IT infrastructure, something the Lieberman bill would not require.

Controversially, the Lieberman bill would also create a framework for the President to authorize emergency measures to protect the nation's most critical infrastructure if a cyber vulnerability is being exploited or is about to be exploited. Critics characterize this component of the bill as giving the President an "Internet kill switch."

The Challenge of Competing Interests. Overall, the two cyber bills reflect the Senate committees from which they came. Rockefeller and Snowe both sit on the Senate Committee on Commerce, Science and Technology. Unsurprisingly, their proposed legislation leans heavily on the private sector, with a healthy leavening of authority relating to the Department of Commerce.

Senators Lieberman, Collins, and Carper all sit on the Senate Committee on Homeland Security and Governmental Affairs. Consequently, their proposal considers cyberspace through the prism of critical infrastructure protection, relying on existing capabilities within DHS.

Concerns about cyberspace are bigger and broader than the parochial concerns of Senate committees. In the end, the right answer will involve strengthening the leadership of all loci of response: DHS, Commerce and the private sector, and others with the capability to respond to a cyberattack, like the Department of Defense. Before Congress acts, America needs a broader cybersecurity legislative conversation.

Moving Forward. Rather than trying to forge comprehensive legislation from narrow perspectives, Congress might broaden the scope of its efforts while tackling the cyber challenges in more manageable components.

1. Knowing what is going on online (situational awareness) and early warning are vital. Strengthening these capacities ought to be the first priority.
2. Much more attention needs to be given to building human capital—the cyber-strategic leaders with the right skills, knowledge, and attributes to do the job—rather than just reorganizing or creating more bureaucracy.
3. In the wake of the failed collaboration between the White House and BP in responding to the Gulf oil spoil, it is clear that America needs much more hard thinking over how to build resilient public–private partnerships.
4. Any legislation that addresses these cybersecurity issues should ensure that the liberties, privacy, and economic freedom of Americans are protected.
5. The issue of the emergency powers granted to the executive requires a full and extensive assessment.

No Silver Bullet. There is no silver-bullet law that will solve all cybersecurity challenges. Nor is there a permanent solution, as the cyber universe is a dynamic environment. Legislators will have to pay attention to new technological trends and developments in the wired world to stay current.

Congress is only just beginning to take cybersecurity seriously. When it begins to act, it should ensure that its directives make cyberspace better, not worse.

*—**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 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.*