WebMemo
Published by The Heritage Foundation
No. 1684
October 31, 2007

Grading Cybersecurity Initiatives: Six Necessary Components

James Jay Carafano, Ph.D.

A recent denial-of-service attack on government and private sector computer systems in Estonia has spurred renewed interest in cybersecurity. The Bush Administration is preparing to unveil a major "Cyber Initiative" designed to thwart malicious acts by states or transnational threats. Congress is pressing for details and consultation on the plan, and the House Homeland Security Committee recently announced the creation of a commission to study the government's proposals. As these efforts get underway, Congress and the Administration need to ensure that their initiatives meet *all* of the nation's priorities: enhancing security, promoting economic growth, and preserving the liberty and privacy of American citizens and respecting those of our friends and allies.

The initiatives that will likely best serve the United States and its international partners in the cyber conflicts of the 21st century are those derived from private sector experience, emerging military and intelligence capabilities for conducting information warfare, and law enforcement measures for combating cyber crime. The U.S. needs a national framework that builds on these capabilities, encouraging them to collaborate and reinforce one another. These initiatives should include:

- **Adopting best practices.** Both government agencies, such as the National Institute for Standards and Technology, and the private sector continue to develop best practices and lessons learned. These can be effective tools. Ensuring that these are refreshed 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 up with determined and willful efforts to overcome security efforts.
- **Employing risk-based approaches.** All information programs must include assessments of criticality, threat, and vulnerability as well as measures to efficiently and effectively reduce risks.
- **Fostering teamwork.** Cybersecurity is a national responsibility requiring international cooperation. The United States must maintain effective bilateral and multinational partnerships to combat cyber threats. These efforts should include rigorous measures to prevent the export of sensitive technologies to malicious actors, as well as persistent vigilance to ensure that adversarial states and transnational terrorist and criminal groups do not penetrate U.S. companies that provide essential capabilities and sensitive national security services.
- **Exploiting emergent private sector capabilities.** These may come from many sources, such as small companies and foreign countries. The U.S. government must become a more agile consumer of cutting-edge commercial capabilities.

This paper, in its entirety, can be found at:
www.heritage.org/Research/HomelandDefense/wm1684.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

- **Focusing on professional development.** Most government information programs underperform because, due to inattentive senior leadership, they lack clear requirements and hold unrealistic projections of the resources required to implement those requirements. Such problems can be addressed by maintaining a corps of experienced, dedicated service professionals. National security professionals must have familiarity with a number of diverse security-related disciplines and practice in interagency operations, working with different government agencies, the private sector, and international partners. These skills and attributes must include expertise in cyber operations as well as in developing and managing new systems.
- **Developing robust offensive capabilities** to respond to cyber attacks and malicious acts by either state or non-state threats using the full range of military, intelligence, law enforcement, diplomatic, and economic means.

Washington can do better in preparing to respond to current and future cyber threats. What is needed, however, is not massive reorganization, massive government bureaucracy, massive infusions of government cash, or massive intrusions into the marketplace and the lives of Americans. What is needed is long-term commitment and sound initiatives based on better and faster acquisition of commercial services; better and smarter management of military, intelligence, and information technology programs; and better and sustained professional development of federal, state, local, and private sector leaders.

—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 at The Heritage Foundation.