Commentary

Group effort needed to secure cyberspace

By CHRIS BRONK, DAN CASTRO and DAN WALLACH

June 14, 2009, 4:36PM

The Internet is not broken, but it could be. Protecting the nation's computer and communications networks from attack remains a challenge. Day after day we are bombarded by stories of data breach and potential vulnerability in our national information infrastructure. Addressing this issue and following up on a campaign pledge, the Obama administration has conducted a 60-day review, completed in April, of our national cybersecurity posture. Led by Melissa Hathaway, a former consultant and senior staffer at the Office of the Director of National Intelligence, the review was designed to set the stage for a "strategic vision" on cybersecurity. Key to that vision is creation of a cybersecurity coordinator position in the White House, linked to the National Security Council, but also economic advisors.

Clearly applicable to the cybersecurity "czar" position is the aphorism, "Vision without resources is but mere hallucination." We should recall the most common critique of the "Drug Czar" job, once a cabinet-level position. Without an agency to run, the director of the Office of National Drug Control Policy typically held little sway over those doing the work at the DEA and FBI. This should be remembered. Although many agencies contribute to cybersecurity, including the departments of Commerce and Homeland Security, the largest and most capable government organ in the domain is the National Security Agency (NSA). Shrouded in secrecy, the NSA is big — employing tens of thousands, an estimate, as the actual number and the agency's budget remain classified — and holds enormous material and intellectual resources. That said, the NSA can't handle the job alone. The reality is that cybersecurity is a problem for anyone who writes software, employs a digital supply chain management system, stores electronic medical records, or chooses to use the Internet. It is an individual and organizational responsibility. Wisely, the Obama administration has recognized this complexity and the concomitant need for public-private partnership on the issue.

That the White House is willing to expend effort on cybersecurity is terrific news. However, the federal government has had enormous difficulty in securing its own computer networks. It cannot make cyberspace more secure without significant input from industry, academia and the population at large. While one pundit quipped that Oprah Winfrey should broadcast an episode on the topic and give away free Internet security software to her massive audience, the truth is, such a suggestion is not a bad idea. A national cybersecurity strategy will require buy-in from the broader public, not just government and technology insiders. Teleworking, the BlackBerry and videoconferencing have each changed the way America works and for many, life without information technology is unimaginable. We have heard plenty of bleak prognostication on Internet security, "Digital Katrina" being the latest

rhetorical flavor of the month, but big thinking on the topic is required nonetheless.

Cyberspace is an ecosystem, composed of billions of users, machines and lines of software code. To have government control such a thing is as nonsensical an endeavor as the Communist command economy. Sure, a cybersecurity czar will help, and industry working with government in public-private partnerships is a must, but policy needs to take a long-term view. Government's key role should be in doing again what it did before in the crafting of the Internet from 1969 to 1992, providing investment to drive innovation. While monitoring cyberspace should continue, government and industry working together to detect vulnerabilities and mitigate them, the cyber czar should serve as the chief advocate for a safer, more secure global information network and the lead secure IT buyer for the sector's largest single customer, the U.S. government. The job will entail keeping research oriented agencies, both military and civilian, focused on the cybersecurity issue and appealing to Congress for the necessary funding.

Market forces aside, government will also need to govern in cyberspace, partnering with others to construct new rules and regulations. The job will require reaching out to foreign counterparts, especially from the world's most developed and, therefore, most vulnerable nations, as the problem of cybersecurity does not begin and end at the borders of the United States. But what must be resisted is the temptation to push the cybersecurity challenge strictly into the highest level of the U.S. national security agenda.

This is not a job that the Pentagon or intelligence community should choose to go it alone on. As the United States continues along a path of digital transformation and builds new digital infrastructure such as a "smart" energy grid and electronic health records, cyber security will be a critical issue for all government agencies. Certainly the NSA will be needed at times, but often it will not. The departments of Commerce, Justice, Homeland Security as well as non-government players, from network operators to software and hardware developers, should provide the knowledge and resources called for in mitigating threats to what has become the critical infrastructure of our nation's critical infrastructures, the national information grid. For now, the cyber coordinator's most important job will be to create the strategy that determines which government agencies and industry partners are needed to handle each major vulnerability or incident.

Wallach is an associate professor of computer science at Rice University. Castro is a policy analyst at the Information Technology and Innovation Foundation in Washington, D.C. Bronk is a fellow at Rice's James A. Baker III Institute for Public Policy.