

## *NATIONAL SECURITY: Cyber-Safety Goes Global*

The Bush Administration is moving quickly to fill the gaps in its plans to protect critical U.S. infrastructure systems such as telecommunications, financial services, and transportation. But private-sector Internet-security experts say the Administration may be overlooking the fact that these systems can be disrupted by attacks launched over the Internet, and that vulnerabilities in the Internet often lie outside U.S. borders.

"The Office of Homeland Security has been occupied with responding to the terrorist attacks," said Bruce McConnell, the former head of the International Y2K Cooperation Center. "They have not had time to develop a concrete, proactive program to address international cyber-security."

But the State Department's Michele Markoff, senior coordinator for international critical infrastructure protection outreach policy, said this week that international efforts have "absolutely not" taken a backseat to domestic security issues. Markoff is at the epicenter of the Administration's international efforts and is working under John Bolton, undersecretary of State for arms control and international security. "What 9/11 has done is crystallize the interest in cyber-security," Markoff said. "If anything, it has speeded up our efforts."

Since September 11, Markoff's office has helped coordinate several lengthy meetings on networked critical infrastructure with nations sympathetic to U.S. concerns. It has also begun prioritizing new proposals and has received several communications from other countries on the need to act on cyber-security, she said.

An October 16 presidential executive order created a senior executive board on critical infrastructure protection; Richard Clarke, the President's chief adviser for cyber-security, will chair the board. On international issues, the order called for the board to support the State Department in its efforts to coordinate U.S. government programs for international cooperation on cyber-security.

The order also called for the creation of a standing committee on international affairs, chaired by a designee of the Secretary of State, who is expected to be Bolton. "The executive order codifies State authority, so we are able to direct this even more avidly," Markoff said. "It's trying to give us teeth." Many agencies have ad hoc groups that address international security issues, and State's job is "to weave together the very different strands of government involvement," she said.

Markoff's office also works through the United Nations and other forums to raise awareness of cyber-security issues among developing countries. "I think there's an international hunger for knowledge," she said. She also stressed that the cyber-crime

treaty completed this fall by the 43 members of the Council of Europe and the United States could help address the absence of cyber-crime laws in many countries. The United States has not announced whether it will sign the treaty at the ceremony in November. Contingency plans put in place in preparation for the year-2000 computer bug helped restore the failed telecommunications networks and stock exchanges during the week of September 18. Now, the Y2K center, shuttered in March 2000, is gaining new attention as a possible model for international cyber-security. "A lot of prophylactic measures for Y2K have had a huge role across all the keystone sectors," said Michael Aisenberg, director of public policy at Internet-security company VeriSign Inc. "Query whether we can expect the same level of security practices abroad. It's an endorsement for the kind of hygiene of Y2K."

Harris N. Miller, president of the Information Technology Association of America, has been pushing the idea of creating a Y2K-like center for cyber-security. He recommends that Clarke's office name someone who will focus exclusively on international developments and set up the center.

Bruce McConnell, now president of high-tech consulting group McConnell International, is embarking on a study of global cyber-security practices. Due out early next year, his research will look at laws, information-sharing, the possible need for a Y2K-style center, and individual nations' approaches to cyber-security. The Y2K center allowed countries to share information about cyber-threats confidentially, McConnell said. A bill introduced on October 9 by Sen. Robert Bennett, R-Utah, would suspend the Freedom of Information Act in times of threat to the nation's critical infrastructure, thereby encouraging information-sharing.

But private-sector groups may not be ready to share very much with their foreign counterparts. At a board meeting of the industry-government Partnership for Critical Infrastructure Security last week, a British proposal to develop a bilateral relationship met with reticence.

The nonprofit Internet Security Alliance, a joint venture of the cyber-security response team CERT Coordination Center and the Electronic Industries Alliance, was set up in April to operate above the limitations of the existing "stovepipe," or sector-specific, government advisory structure. CERT also is part of the international Forum of Incident Response and Security Teams.

"Right now, there is a national-security compulsion" in the United States, said Aisenberg. "But it's naive of us to think it's all red, white, and blue. U.S.-derived interests based on financial and other economic considerations ... simply may not be exportable to the rest of the world."

William New is a senior writer for National Journal's Technology Daily.

William New  
National Journal