Oh What a Tangled Web We've Wed
Don Wolfensberger
Introductory Essay
For Congress Project Seminar
Congress, the Executive and the Cyber Threat
Monday, May 17, 2010

The speed and interconnectivity of the Internet is both its greatest strength and its greatest vulnerability. The Net is probably the single most visible symbol today of what is meant by globalism—the free flow of people, ideas and information across geographic and political borders. Despite the invention of all manner of safety mechanisms to protect computer networks from cyber attacks aimed at stealing, altering or deleting information or at disabling systems altogether, new threats seem to emerge daily that circumvent or overcome these defensive devices.

Given the dependence of modern societies on electronic communications to function—spanning the gamut of business, government, transportation, power, water, healthcare, financial and military systems—it is not surprising that government should take a very intense interest in developing policies aimed at preventing cyber attacks that can effectively shut down not only a country, but potentially the entire world economy.

Building on the initiatives of the previous administration, Congress and the Executive Branch are currently engaged in an all-out effort to further identify the nature of the cyber threat and organizational and policy responses to it. Because cyber threats potentially endanger every nook and cranny of private and governmental activities in advanced countries around the world, any effective strategy to counter them will require a multi-pronged domestic and international response.

If ever there were a system that truly is "too big to fail," it is the massive, interconnected electronic network upon which so much of daily life, commerce and governance on this globe depend. With threats and attacks emanating from thousands of state and non-state actors of varying motives and capabilities, it is clear people at all levels of society must be enlisted as part of any effective response to the threat. National governments can provide some of the leadership and resources in this effort, but governmental efforts alone are bound to fall far short of providing an effective deterrent and response.

Background

In January 2008, the Bush Administration issued a secret directive establishing the Comprehensive National Cybersecurity Initiative (CNCI) that created a multi-pronged approach for the federal government to pursue in identifying current and emerging cyber threats. The approach envisions both reinforcing the resistance of existing and future telecommunications and cyber activities against attack, but taking preemptive measures against those threatening to steal manipulate protected data on federal information systems.

That same year, the Center for Strategic and International Studies (CSIS) created a Commission on Cybersecurity for the 44th President to provide advice to the new Administration on creating and maintaining a comprehensive security strategy. The Commission reported is findings and recommendations in December 2008, calling among other things, for a comprehensive national cybersecuirty strategy, a new public private partnership, modernization of legal authorities, and leadership from the White House.

Building on the CNCI and CSIS efforts, President Barack Obama Administration ordered the National Security Council and Homeland Security Council in February 2009 to conduct a "top-to-bottom review of the federal government's efforts to defend our information and communications infrastructure" to ensure the CNCI is being properly integrated, resourced and coordinated with Congress and the private sector. On May 29, 2009, the President announced "a new comprehensive approach to securing America's digital infrastructure" based on the review's recommendations of the best ways "to secure our networks as well as our prosperity."

According to the President's announcement, at the heart of the new policy is the treatment of the country's digital infrastructure—the networks and computers upon which we depend daily—"as a strategic national asset," the protection of which "will be a national security priority." To carry out this mission, the President announced the creation of a new Office of Cybersecurity at the White House to be headed by a Cybersecurity Coordinator.[1]

According to the May statement, the Coordinator would have regular access to the President and advise on a wide range of issues from military cyber defense to coordinating federal security policies. Moreover, the coordinator would be a staff member on both the National Security Council and the National Economic Council. In addition, the Coordinator would work with the Office of Management and Budget to ensure that agency budgets reflect the new cybersecurity priorities and that their responses are coordinated across government in the event of a cyber incident or attack; and with the government's Chief Technology and Chief Information officers to ensure accountability for making cybersecurity a key management priority within federal agencies; and for working with state and local governments and the private sector to ensure an organized and unified response to future cyber incidents.

To carry this out, public-private partnerships will be forged to find technology solutions to ensure security and promote prosperity, without government dictated security standards for private companies. And, a national campaign will be launched to promote cybersecurity awareness and digital literacy. Integral to the success of all these efforts, the President emphasized, is an ongoing dedication to the protection of personal privacy and civil liberties.

Despite urging from many in Congress and in the private sector to move quickly on the appointment of a Cybersecurity Coordinator, it wasn't until December 22, 2009, that the President named Howard A. Schmidt, a cybersecurity expert from the previous Administration, to the position. The announcement, made through a White House e-mail message from John Brennan, the President's counterterrorism assistant, omitted any mention of Obama's earlier

[1] Remarks by the President on Securiing Our Nation's Cyber Infrastructure, The East Room, May 29, 2009, accessed at http://whithouse.gov/the-press-offce/remarksk-president-security-our-nations-cyber.... on 5/10/10.

pledge that the Coordinator would serve on the staff of the and National Economic Council (as well as on the NSC staff). It did indicate, however, that he would be "a key member of [the President's] National Security Staff" and "will also work closely with his economic team…."[2]

Congress's Role in Cyber Policy

The White House "Fact Sheet" accompanying the President's announcement in May asserted that, "We must make cybersecurity a national priority, and lead from the White House." No specific legislative requests or recommendations were made as part of the President's statement or in the summary of the review team's report (even though the original charge to the review panel was to seek ways to integrate the efforts of Congress, the Executive and the private sector.) Nor, for that matter, was the Congress even mentioned in either document. [3]

However, it seems clear from the nature of the changes being contemplated that some statutory changes and funding priority shifts will be necessary to facilitate implementation of the recommendations. Regardless, if post-9/11 activities on the Hill are any indicator, Congress will surely be conducting ongoing oversight of the cyber activities being carried out in the Executive Branch in fulfilling its powers over the purse strings, and those inevitably lead to legislative policy prescriptions.

Indeed, on March 24, 2010, the Senate Commerce, Science and Transportation Committee ordered reported The Cybersecurity Act of 2009 (S. 773), sponsored by Commerce Committee Chairman John D. Rockefeller IV (D-W.Va.) and cosponsored by Committee Member Sen. Olympia Snowe (R-Maine). (Both Senators are also members of the Senate Intelligence Committee.) The purpose of the bill is "to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications…." According to one news account of the legislation, its actual purpose "is to prod the Obama administration and Congress to be more aggressive in crafting a national strategy for dealing with cyberthreats." It would do so by ….

The two Senators are also sponsors of "The National Cybersecurity Advisor Act" (S. 778) which would elevate the current Cybersecurity Coordinator's job to a Senate-confirmed, cabinet-level position to lead national efforts to protect the country's computer systems. A similar bill was ordered reported May 5, 2010, by the House Oversight and Government Reform Committee's Subcommittee on Government Management, Organization and Procurement." Introduced by the subcommittee's chairwoman, Rep. Diane E. Watson (D-Calif.), "The Federal Information Security Management Act of 2010" (H.R. 4900) would established a National Office for Cyberspace in the Executive Office of the President, and makes ifs director subject to Senate

[2] "Introducing the New Ckybersecurity Coordinator," The Whie House Blog, posted by Macon Phillips on December 22, 2009, at 7:30 a.m., accessed at http://www.gov/blog/2009/12/22/intordcing-new-cybersecurity-coordinator> on 5/10/10.

[3] Perhaps tellingly, of the 20 persons attending the President's May 29, 2010 cybersecurity announcement only two were Members of Congress: Rep. Bart Gordon (D-Tenn.), chairman of the House Science and Technology Committee; and Rep. Peter King (R-N.Y.), ranking Republican on the House Homeland Security Committee. Most of the other attendees were executive branch officials. News report, text of president's announcement, White House fact sheet and list of attendees accessed at <http://www.boston.com/news/politics/politicalintelligence/2009/05/president_annou.html >on 4/9/2010.

confirmation. The bill also requires agencies to utilize automated monitoring capabilities to assess their vulnerabilities to cyber threats.

Meantime, the House of Representatives passed the "Cybersecurity Research and Development Act Amendments of 2009" (H.R. 4061) on February 4, 2010, by a vote of 422-5. The bill, sponsored by Rep. Daniel Lipinski (D-Ill.), was ordered reported by the House Science and Technology Committee the previous November. Its stated purpose is, "to advance cybersecurity research, development and technical standards." According to the Majority Whip's packet for the day of consideration, the Office of Management and Budget did not issue a "Statement of Administration Policy (SAP) on the bill.

It is clear from the host of cybersecurity legislation introduced in the last two Congresses that jurisdiction responsibilities for cybersecurity remain as diffuse among multiple committees and subcommittees as was the larger counterterrorism issue for which the 9/11 Commission was so critical. If anything, there has been a proliferation of subunits in Congress with the terms terrorism, homeland security, and cybersecurity since the 9/11 Commission called for greater consolidation. In an effort to address this ongoing tangle of jurisdictional lines, the Senate Committee on Homeland Security and Governmental Affairs undertook an effort in late 2009 to combine forces with the Armed Services, Commerce, Intelligence and Judiciary committees to develop comprehensive cybersecurity legislation.[4]

In addition to special legislation addressing various aspects of cybersecurity, the subject is regularly dealt with in the ongoing defense and intelligence authorization bill as well as in their Appropriations Committee counterparts.

Conclusion

If it seems that so much of what is going on in government on the cybersecurity front is under the radar, it's because much of it intentionally is for security reasons. At the same time, what does get out is not terribly reassuring over what little progress being made organizationally or from a policy standpoint. The same problems that have plagued our counter-terrorism/homeland security responses generally, are writ large when it comes to cybersecurity because it involves so many systems and players both in an out of government and around the globe. It is difficult to determine how much of the problem in addressing this issue is grounded in turf battles and differing cultures among federal agencies and congressional committees and how much is due to the rapidly changing nature of the technologies involved and the challenge of ever getting a proper handle on them. The answer is probably both, and that only compounds the degree of difficulty in getting things right. It is easy to suggest that leadership on the issue must emanate from the White House but quite another to carry it out given all the existing policy czars elbowing each other for attention and resources. Moreover, Congress must also play a lead role in fashioning any comprehensive policy, and it is not easily led or even moved. It would be tragic if it took a cyber-9/11 before an effective policy and organizational framework could be forged.

[4] "Catherine A. Theohary and John Rollins, "Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress, CRS Report for Congress (R40836), Sept. 30, 2009, 10, accessed at http://assets.opencrs.com.