CyberPro

July 26, 2011

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: CONGRESSMAN JIM LANGEVIN (D-RI)

NSCI's Charles Winstead recently had the opportunity to interview Congressman Jim Langevin. Throughout his career, Congressman Jim Langevin has made Rhode Island's priorities his own and fought to open the doors of government to its rightful owners - the people of this great nation. Recognized as a national and party leader on national security, health care and stem cell research, Congressman Jim Langevin has dedicated his many years of public service at the federal and state levels to the hard-working citizens of Rhode Island. Langevin serves on the House Armed Services Committee, where he is Ranking Member of the Emerging Threats and Capabilities Subcommittee, and serves on the Subcommittees on Strategic Forces and Seapower and Projection Forces.

Securing our nation's technology infrastructure against cyber attack is a top priority for Langevin, both within and beyond his committee work. As the Co-Founder and Co-Chairman of the bipartisan House Cybersecurity Caucus, he has taken on a leadership role in raising awareness of cybersecurity issues in Congress and fostering dialogue and debate on the critical questions surrounding this topic. In addition, he is working to implement the recommendations of the Center for Strategic and International Studies (CSIS) Commission on Cyber Security for the 44th Presidency, which Langevin co-chaired. He is encouraged that the President understands these modern security challenges, and is working closely with the Administration to ensure that the Commission's recommendations are considered as a national security agenda is developed.

NSCI: You have obviously taken cybersecurity very serious. Do you have any thoughts on how we get more Congressional members "up to speed" on cybersecurity so our national policy decision-makers are more informed?

LANGEVIN: In 2008, I co-founded the bipartisan Congressional Cybersecurity Caucus in large part because of the need to increase awareness about our significant shortcomings in this area and their impact on our national security. We have made significant progress by bringing federal officials, outside experts and private companies to Capitol Hill to brief members of Congress and their staffs, and new strategies and legislative proposals coming out of the White House and Defense Department have also helped raise the issue's profile. The challenge now is translating this heightened interest into action. We will come up with much better solutions for everyone involved, including government, military, industry and consumers, if we take action before a major cyber disruption happens rather than reacting after the fact.

NSCI: Several have noted the numerous cyber-related bills introduced or supported in Congress, the overlap of committee jurisdictions regarding cybersecurity, and the lack of cybersecurity legislation making it into actual law and/or policy. Will the President's recent cybersecurity legislative guidance help?

LANGEVIN: The White House's proposal was an important step that has helped move the process forward. We have seen more movement in Congress toward legislation since its release. The overlap of committee jurisdictions continues to be an issue that could unnecessarily slow down the process. At the same time, I am encouraged that many Members want to take action. My priority is to ensure that we end up with as comprehensive a bill as possible and that its substance meets the extraordinary challenges we face.

NSCI: Speaking of the President's recent cybersecurity legislative guidance, what are your thoughts on it and other cyber-related White House proposals?

LANGEVIN: The Administration's recommendations make significant progress in a number of key areas, while others may need to be strengthened by Congress. Perhaps most importantly, it has been helpful for Congress to have the President's perspective, and I hope it will be a catalyst for more action.

Two important advances in the President's plan are national data breach requirements that keep customers informed when their private information is stolen or exploited, and increased penalties and definitions for cybercrime. These efforts will go a long way in combating effects of the large-scale breaches making headlines every month. In addition, the White House plan makes progress toward protecting critical power, water, telecommunications and financial infrastructure, and increasing information sharing. The government has a very detailed view of specific advanced threats, but we don't have the broad visibility that our Internet Service Providers (ISPs) do. The White House proposal tries to decrease the barriers for sharing information on specific cyber threats so that the private sector and the government can better protect themselves.

However, I was disappointed that the Administration did not include a strengthened White House office for cybersecurity coordination. Howard Schmidt has done an excellent job handling cyber policy for the executive branch, but the changes we need will require a White House director, confirmed by the Senate, with the budgetary authority to require government agencies to protect themselves. This director, as I and some of my Senate colleagues have proposed, would also be able to work with the owners of critical infrastructure to better coordinate with government efforts and requirements.

Both the Executive and Legislative branches have been very supportive of cybersecurity education aimed at increasing the quality and quantity cybersecurity workforce. Can you tell us about any metrics that help let Congress know our cyber workforce is improving? Are there metrics being used or developed for other cybersecurity areas such as the security of our critical infrastructure, small-medium sized businesses, defense industrial base, etc?

LANGEVIN: Even our best ideas about strengthening cybersecurity won't amount to anything without the talent to execute them. Unfortunately, our country is not training nearly enough people to contribute. In a report earlier this year by the CSIS cybersecurity commission that I co-chaired, we noted that little has been done to address this shortage and we must start tracking more effectively the number of people graduating with the abilities to improve cybersecurity. That tracking must include measuring how many experts can work with the industrial control systems used in critical infrastructure.

In addition to making this a component of my comprehensive cyber legislation, I have been working with educators in my home state of Rhode Island to develop models for producing qualified cyber professionals. We recently launched one of the first High School Cyber Challenges to foster computer security skills by testing youth in a competitive setting and encouraging them to think about a cyber career. I also commissioned a cybersecurity symposium at the University of Rhode Island, which has led to the development of a Cyber Center of Excellence to increase the number of graduates with skills in this area.

NSCI: In addition to education, you've supported increased awareness of cybersecurity threats, vulnerabilities, and steps to minimize the risks. How should Congress help with this to ensure increased awareness efforts target policy makers, large and small businesses, law enforcement, home users, students, and others who have a role to play?

LANGEVIN: Members of Congress are in a unique position to engage all of these constituencies by regularly discussing the important role of cybersecurity in so many aspects of our lives. We should also encourage efforts similar to the Rhode Island Cyber Disruption Team that I helped unveil this month, which combines the abilities of law enforcement, state government, businesses and educators to prevent and respond to threats of cyber disruptions and intrusions, particularly to the state's critical infrastructure.

NSCI: The House seems to be showing particular attention in protecting our critical infrastructure, specifically the electric grid. Meanwhile, some say we are reaching a point of diminishing returns when it comes to cyber defense. What is needed to ensure we strike the right balance between cyber offense and defense? How does the offense / defense balance differ between critical infrastructure and other areas dependent on the Internet?

LANGEVIN: Our priority needs to be closing the vulnerabilities in our critical infrastructure and the networks that store sensitive information. As a member of the Armed Services Committee, I am continuing to press for greater clarity about what authorities DOD requires to carry out its defense of

our military networks and support ongoing operations. The strategy recently released by the Department of Defense begins to define the Pentagon's role, but there are some key areas where we must continue to flesh out answers. Specifically, what are acceptable red lines for actions in cyberspace and what resources can and will the Defense Department provide to the Department of Homeland Security (DHS), private companies, and international partners to enable their own defense? Does data theft or disruption rise to the level of warfare or do we have to see a physical event, such as an attack on our power grid, before we respond militarily?

NSCI: Can you tell us about any policies and/or incentives aimed at industry and individuals improving their cybersecurity (e.g., tax breaks for the purchase of antivirus software)?

LANGEVIN: Current legislative efforts are exploring effective incentives and their costs and benefits. We should only compel people to act in limited circumstances, which I believe mainly extends to our government, military and critical infrastructure. In the case of critical infrastructure, many entities have not paid serious attention to threats and their potential impact on large numbers of Americans. We need to consider a combination of carrots and sticks to ensure they are protected, and I am working on further proposals to that effect.

NSCI: Many view the internet as inherently insecure and believe we may in fact need to start over, perhaps by having one type of system that is more open and a second system that is more secure. Are you aware of any Congressional discussions and/or hearings related to this and if, or how, Congress should help move things in this direction?

LANGEVIN: While much of our cybersecurity discussion focuses on the threats the Internet has facilitated, we cannot forget that it is an incredibly powerful tool that has revolutionized every part of our society. There are not any serious efforts to dismantle it, nor should there be. If we accept the need to take steps that protect our economy and our people from potential damage caused by bad actors, we can work with the system we have and take advantage of its limitless possibilities.

NSCI: Final question, unless you have something to add that we haven't covered. Government can always do more, but what is your sense about how much the people want government to do in terms of cybersecurity?

LANGEVIN: As we work to protect our assets from cyber disruptions and intrusions, everyone involved must take great care that personal privacy is protected. We can overcome concerns by engaging the American people in a continuous dialogue about threats we face and steps taken to protect them. At the same time, we must ensure our actions are transparent and show that any regulations are limited. I believe privacy concerns highlight the importance of taking action now. History has taught us that we are prone to overreact after an incident that causes great damage. It is critical that we put in place effective and responsible policies before that happens.

NSCI: Is there anything else you'd like to add?

LANGEVIN: Thank you for the opportunity to communicate with your readers about this subject. As I mentioned above, transparency is a vital part of improving our cybersecurity, and I want to take every chance to engage as many communities as possible about what needs to be done. I welcome any feedback.

NSCI: Thank you very much for taking the time to visit with us.