National Security Cyberspace Institute NSCI

# CyberPro

April 21, 2011

Keeping Cyberspace Professionals Informed

## SENIOR LEADER PERSPECTIVE: CONGRESSMAN RANDY FORBES (R-VA)

*NSCI's Charles Winstead recently had the opportunity to interview Congressman Randy Forbes. Since his constituents elected him to Congress in 2001, one of Randy's key priorities has been to protect and defend our nation. Randy is a member of the Judiciary Committee and the Committee on Armed Services. As Chairman of the House Armed Services Readiness Subcommittee, Randy is tasked with ensuring that our men and women in uniform have the equipment, facilities, and training to be the most effective military in the world. Randy is also a member of the Congressional Prayer Caucus, Congressional China Caucus, Congressional Modeling and Simulation Caucus, and the House Cybersecurity Caucus. Randy founded and chairs the Congressional Prayer Caucus and has led this group of bipartisan Members in national efforts to protect prayer and our nation's spiritual history. He is known as a skilled orator on the Judiciary Committee and, as the former Ranking Member of the Crime Subcommittee, Randy is often called upon to lead the debate on national issues such as gang crime or immigration reform. As founder and chairman of the Congressional China Caucus, Randy has introduced legislation to combat Chinese espionage and is frequently tapped as a national commentator on Sino-American relations. Groups as diverse as the US Chamber of Commerce, the NAACP, the National Taxpayers Union, and the American Farm Bureau Federation have all recognized the work Randy has done in Congress - a testament to Randy's independent problem-solving and focus on bipartisan solutions. Randy places a high-priority on partnering with community leaders and elected officials of all political persuasions to bring about greater economic prosperity, increased educational opportunities, safer communities, and improved local transportation and infrastructure for the Fourth District.*

**NSCI: You recently announced becoming a member of the House Cybersecurity Caucus. Can you tell us about this Caucus and what we can expect to see from it this year?**

**FORBES:** The purpose of the Cybersecurity Caucus is to actively create dialogue among members of Congress to identify challenges and make recommendations on cybersecurity. Over the next year, I believe it is important that we not only continue to create dialogue, but really work to bring it to the forefront in Congress. Now more than ever, it is important that we draw attention to the need for a cybersecurity plan and that we help policymakers gain an adequate understanding of the resources necessary to get us there.

**NSCI: You co-chair the Congressional Modeling and Simulation Caucus. What role do you think modeling and simulation should play in improving cybersecurity?**

**FORBES:** The great thing about modeling and simulation is that it allows us to prepare and train for all kinds of scenarios before they even happen. The military has recognized the potential of this technology, and they regularly use it to train our men and women in uniform to ensure they are acclimated and ready for theater. In fact, Secretary of the Army, John McHugh, testified just recently in an Armed Services Committee hearing that modeling and simulation is an absolutely essential technology. I could not agree more. Especially at a time when we are facing both the realities of significant budget constraints and twenty-first century warfare – including cyberwarfare – modeling and simulation has great potential. The technology will allow us to train and prepare for potential cyber threats before they happen, enabling us to have the processes in place to respond quickly if we ever face a cyber attack.

**NSCI: We've seen numerous pieces of cyber-related legislation introduced over the last few years, but we seem to have little to show for it in terms of a more secure cyberspace. How do you think we fix that?**

**FORBES:** Again, I believe it begins with creating dialogue among members of Congress on the importance of cybersecurity. As a member of the Armed Services Committee we are taking this threat very seriously and will be investigating the impact of cyberattacks on the United States military to begin to take proactive steps at developing a strategic cybersecurity plan. As the Chairman of the Readiness Subcommittee, I plan to be actively engaged in these developments.

**NSCI: As Chairman of the House Armed Services Readiness Subcommittee, how would you assess our military's cybersecurity equipment and training? Are there any specific actions you would like to see Congress and/or the military take to improve their cybersecurity readiness?**

**FORBES:** Cybersecurity capabilities of the U.S. military are largely classified, but the newly established U.S. Cyber Command is working hard to ensure we can defend our vital defense networks against a variety of threats. One major concern, however, is China's increased interest in developing offensive cyber capabilities and its impact on our military readiness. Without adequate protections in place, our vital military communication and logistic networks could be at risk.

Cyber espionage is a growing threat to our military readiness. In 2009 the Department of Defense reported that a cyber attack, appearing to have originated from China, successfully stole design and electronics information on the F-35 Joint Strike Fighter program. Without putting a spy on American soil, a potential adversary undercut our capability while it was still in the development stage. We have to protect our military development in order to maintain readiness.

Supply chain management is also critical in protecting against cyber threats. With the majority of computer chips being manufactured in China, defense supply chain managers have to ensure that adequate protections are in place so that compromised or counterfeit hardware is not installed in critical communication and logistic IT systems.

We have the difficult position of having to defend and to be 100% perfect in defending against every cyber attack, while the attackers only have to get it right once. Our military must be trained and ready for operations in a reduced capability environment so we can be sure our forces can adapt to adverse conditions created by cyber attacks. Over the next year and as cybersecurity threats increase, it will become more and more important for Congress to make it a priority to hear directly from our military commanders, both on their assessment of the state of our cybersecurity readiness and the tools that they need to ensure we are prepared to face these cyber threats.

**NSCI: In your recently released "The Caucus Papers: A Conversation on China", you discuss cyber warfare and alleged Chinese attacks on U.S. government and industry. What are the top 2 or 3 things you think Congress can do to help in this area?**

**FORBES:** First, we need to develop a whole-of-government state-of-the-art strategic cyber defense plan. According to the Government Accountability Office, one of the critical challenges for us as we move forward is developing a comprehensive national strategy that specifies overarching goals and a way to measure the success of those goals. Because cybersecurity spans the breadth of the public and private sector, it is important that we create a channel of communication now among business, civil society, and government regarding the challenges we face in cyberspace—spanning international law, privacy and civil liberties, security, and the architecture of the Internet. Congress can, and should, be at the center of that dialogue.

Second, as you alluded to earlier, we must take full advantage of tools available through modeling and simulation to create a cybersecurity system within our agencies that is unrivaled. We can begin by conducting studies to assess the potential use of modeling and simulation to strengthen cybersecurity. Last year, I worked to have an amendment included in the annual National Defense Authorization Act to do just that.

**NSCI: You talked about the need for a "whole-of-government state-of-the-art strategic cyberdefense plan". How comfortable are you with the cybersecurity roles, responsibilities and authorities as currently delineated within our federal government (i.e. Departments of Defense, Homeland Security, State, Commerce)?**

**FORBES:** Last August, the Government Accountability Office released a report stating that the United States' approach to cybersecurity falls drastically short. Among the findings in the report, the GAO noted that there is no coherent plan stating who is in charge at the federal government level. They also noted that national goals have yet to be established in terms of priorities in protecting our cyber systems. While each department may be working towards its own sets of rules, we are missing a huge piece of the puzzle: interagency cooperation. We need additional interagency cooperation to adequately protect the United States in the realm of cyberspace. Until that point, the United States will remain vulnerable to threats emanating around the world.

**NSCI: How would you describe the risk (i.e., threat + vulnerability) of a major cyber attack on U.S. critical infrastructure (e.g., banking, power grid, transportation, defense)? What are the key policy gaps we have in deterring or responding to such an attack?**

**FORBES:** Many individuals do not realize the extent to which cyberattacks could impact us as a nation. The United States is more dependent on our computer systems than any other country – from military readiness to transportation and energy grids to banking systems to national security operations to civilian infrastructure. As you know very well, an online attack of any of these systems could sabotage power plants or financial markets, stop transportation systems, or result in billions of dollars in annual losses to businesses around the globe. These attacks would not just affect the government but would reach American citizens on a very personal level.

I still believe our greatest weakness in cyberspace is our lack of ability to "connect the dots" between agencies. Sharing information is not a matter of courtesy. It is not a favor. It is the duty of our intelligence communities. We have the best resources and best minds in the world working to protect our cyber systems, but the government has to use them effectively each and every time. Interagency cooperation is critical to achieving a zero-mistakes mission.

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