Thompson: Nation Needs to Be Proactive on Cybersecurity

Roll Call
THE NEWSPAPER OF CAPITOL HILL SINCE 1955

- By Rep. Bennie Thompson
- Special to Roll Call
- April 16, 2012, Midnight

While some have tried to argue that any cybersecurity regulation of at-risk critical infrastructure networks would stifle private-sector innovation and growth, the message from the national security establishment is clear and unified: We must take proactive steps to safeguard the nation from the malicious cyberactivity that is draining our intellectual property, harming commerce and threatening the integrity of our infrastructure.

In fact, over the past few weeks, FBI Director Robert Mueller, former Homeland Security Secretary Michael Chertoff and former National Intelligence Director Michael McConnell have gone on the record as saying that the threat to our government and critical infrastructure from cyberattacks is real and growing and that a legislative fix is sorely needed to keep pace and reform our country's cybersecurity efforts.

Speaker John Boehner (R-Ohio) has said comprehensive cybersecurity legislation will come before the House by the end of the month. To address the real and growing cybersecurity threat, any such comprehensive legislation must contain three essential elements.

First and foremost, it must address the cyberthreats to networks controlling critical infrastructure, such as water and power utilities. Such infrastructure is essential to the basic functioning of our society. Vulnerabilities to our electric grid and other critical infrastructure will not be fixed by sharing information alone; proactive steps are needed to build toward a level of security that is commensurate with risk. A tailored approach that puts critical infrastructure owners and operators on a path to meeting basic risk-based standards is essential to ensuring that their networks are protected from potentially devastating cyberattacks. Some have launched a scare campaign against such an approach and have attempted to brand these efforts as excessive regulatory encroachment on the private sector. But the protection of critical infrastructure is, in fact, a national security issue, as evidenced by the active push from President Barack Obama and top defense, intelligence and homeland security officials. The growing threat to our infrastructure necessitates a consensus development of risk-based standards.

Second, the Department of Homeland Security's role as the leader for protecting federal civilian networks and supporting the private sector's cybersecurity efforts must be solidified, not weakened, in any such legislation. Several proposals on Capitol Hill would scale back DHS' role

under the Federal Information Security Management Act, the law governing security of federal government networks. These proposals essentially ignore almost a decade of progress in implementing FISMA, in which DHS has built significant operational capabilities to help secure federal agencies' systems. FISMA reform is urgently needed, and any such reform effort should provide the DHS with the authority needed to fully execute its cybersecurity mission and better enforce security standards across federal networks. Forcing the Office of Management and Budget to take over this effort would be turning back the clock just when the federal government needs to move quicker than ever.

Furthermore, the suggestion that the Department of Defense, particularly the National Security Agency, should take the lead, especially with regard to protecting the private sector, is wholly inappropriate and ill-advised. In fact, the NSA director, Gen. Keith Alexander, recently said that to do so "sends the wrong message." The privacy and civil liberties ramifications implicit in unfettered information sharing between the private sector and the intelligence community preclude such an approach.

Finally, any legislation must promote voluntary information sharing on cyberthreats. It must relax restrictions on the sharing of relevant cybersecurity information between and among the private sector and the government, as well as promote the sharing of cyber-intelligence between the government and the private sector — all while protecting the privacy and civil liberties of Americans who spend a large part of their personal and working lives online. These efforts should be transparent so Americans clearly understand what is done with their information. Accordingly, a civilian federal agency, such as the DHS, must be the central point for such information sharing, and it should put safeguards in place to reduce the likelihood that personally identifiable information about ordinary Americans' Internet activity is shared.

Though these three essential elements are broad, there is reason for concern that, under pressure from special interests, the cybersecurity legislation presented to the House will not meet these basic criteria. However, I believe homeland security should be a bipartisan effort and I believe there is still time to get this right if we come together, as we have done on this issue in the past, to take the steps that we all know are needed to safeguard our country.

Rep. Bennie Thompson (D-Miss.) is ranking member of the Homeland Security Committee.