12-31-2011

President Obama and the Changing Cyber Paradigm

Eric Talbot Jensen
BYU Law, jensene@law.byu.edu

President Obama and the Changing Cyber Paradigm

*By Eric Talbot Jensen**

Among the most important issues for American national security is the national response to the growing threat from cyber activities. This threat is both ubiquitous and potentially catastrophic. It forces the United States, and the entire world, to reevaluate the way in which nations think of both national security and the concept of armed conflict. To combat this threat, President Obama must refocus America's attention, by both reallocating the primary governmental responsibility for cyber security from the Department of Homeland Security (DHS) to the Department of Defense (DoD) and overhauling the public-private partnership that he has made a key component of his cyber strategy.

President Obama's Cyber Emphasis

Beginning with President Clinton in 1996 and continuing through President George W. Bush to President Obama, the Executive Branch has taken the lead on securing the nation from cyber threats but has focused its efforts mainly on government computers and systems. Shortly after entering office, President Obama embarked on a potentially new and expanded view when he called for a complete review of government cyber policies and practices. The report was published several months later.[1] In response to the findings and recommendations of the report, President Obama stated that:

> From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.[2]

President Obama's expanded vision of what the focus of governmental concern should be is undoubtedly correct in that it reflects the reality of today's national security threats. But even this vision is mired in a parochial and anachronistic view of the changing world and its impact on national security.

Changing Threats, Enemies, and Targets

The nature of the changing cyber threat is clearly demonstrated by recent budget decisions in the United Kingdom. During a time of significantly reduced budgets, the UK opted to forgo the production of aircraft for their aircraft carriers and allocate those resources to expanding and maintaining its cyber defenses. The UK is not alone in such decisions. For nations and their leaders, including President Obama, this worldwide attention to the cyber operations reflects a recognition that the types of threats to a nation are changing.

The pervasive nature of the Internet and the increased capability it provides is accompanied by increased risks to nations and users. The Stuxnet malware demonstrates the possibility of a debilitating cyber attack coming from any one of a broad range of actors including other nations, criminal business networks, transnational terrorist organizations, citizen activist groups, flash mobs of like-minded individuals across transnational borders, recreational hackers, and individuals. A new era of threats is emerging and will force the world to look at national security from a different and expanded perspective. President Obama must expand his view to a more holistic approach and be prepared to respond with national power to threats that come from any source.

In addition to expanding views of who may be a national security threat, new considerations as to who or what may be targeted in a cyber attack are also challenging traditional notions of national security. Under current international law, actions that have severe economic effects but do not involve kinetic force do not qualify as a "use of force" that is prohibited by the United Nations Charter. Yet in today's world, surely a cyber operation that destroys confidence in the stock markets of a nation should be seen as a national security threat. The entire international community, and certainly the United States, must adjust how it views an illegal "use of force," recognize that cyber attacks on economic and other similar targets are a potentially debilitating use of force, and commit itself to protection of these assets.

Public-Private Partnership

One of the key findings and recommendations of the Cyberspace Policy Review concerns cooperation between the private and public sector. The report argues that the protection of critical infrastructures, including banking and financial systems, from armed attack is a core responsibility of the federal government. However, in connection with the public-private partnership issue, President Obama stated,

> Let me also be clear about what we will not do. Our pursuit of cybersecurity will not—I repeat, will not include—monitoring private sector networks or Internet traffic. We will

continued on next page

* Associate Professor, Brigham Young University Law School. This is a shortened version of an article that will appear in the Journal of the National Security Forum (forthcoming in 2011).

[2] See http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[2] See http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

> preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free.[3]

This statement by President Obama seems to assume that "open and free" also means to some extent unsecure. That need not be the case; indeed, it should not be the case. On the contrary, keeping the Internet "open" is going to be more and more reliant on increased security measures to maintain the functioning of the World Wide Web.

The government's current approach to public-private partnership is very "hands-off." Even among key defense industries, "there are no regulatory requirements for conducting formal risk assessments,"[4] and U.S. critical infrastructure executives reported the "lowest levels" of government regulation across 14 countries surveyed.[5] It appears that the current public-private partnership means that the private sector does what it wants and the government encourages and suggests security measures but provides no regulation or oversight.

President Obama needs to give serious consideration to the current public-private partnership and begin to assert more regulation over security requirements in the private sector, particularly those that support government operability and critical national infrastructure. To accomplish this, the President should ask Congress to legislate standards of cyber security common to all of these private sectors, with government oversight to ensure the standards are met.

Once the standards are in place, the government should create "red teams" to exercise the security measures of the private sector as they do now with respect to the public sector in order to ensure sufficient security. The results of these exercises should be made public in a "name and shame" effort to help the market drive increased security if government regulation proves less than fully adequate. Such steps are necessary to transform the current public-private partnership from a failed attempt at cooperation into an aggressive pillar of national cyber security.

Allocation of Responsibility

One of the other hallmarks of the U.S. Government's current approach to national cyber security is the designation of DHS as the lead agency to combat cyber threats, with DoD playing a supporting role. Ignoring obvious problems with DHS's ability to fulfill its responsibilities during the previous administration, President Obama has continued to utilize this approach.

As has been previously discussed, the cyber threat is truly a national security issue and though it threatens the homeland, it can originate from anywhere in the world and defies national borders. Assigning the overall responsibility for cyber security to DHS is parochial and ineffective. Instead, DoD ought to be given the lead and allowed to use its current assets such as the National Security Agency, Cyber Command and other agencies which are already heavily engaged in cyber operations overseas to ensure that the cyber security umbrella adequately protects all U.S. assets throughout the world.

A recent report from the Quadrennial Defense Review Independent Panel agrees. The report states:

> In addition, more than 80 percent of the Department's logistics are transported by private companies; mission-critical systems are designed, built, and often maintained by our defense industrial base. The majority of our military's requirements are not neatly bounded by the.mil (dot mil) domain; they rely on private sector networks and capabilities. *That is why the Panel believes it is vital that the Department of Defense ensure the networks of our private sector partners are secured.*

Quadrennial Def. Review Indep. Panel, The QDR in Perspective: Meeting America's National Security Needs in the 21st Century 62 (2010) (emphasis added), *available at* http://www.usip.org/files/qdr/qdrreport.pdf.

Additionally, President Obama must ensure that the cyber activities of DoD and other government agencies are adequately funded, that research is appropriately encouraged, and that the government has aggressive recruiting and pay structures to attract the very best minds in the area of national cyber security. Some of these measures are in their embryonic stages, but more must be done and done more quickly, as U.S. Deputy Secretary of Defense William Lynn recently wrote in Foreign Affairs:

> The United States will lose its advantage in cyberspace if that advantage is predicated on simply amassing trained cyber professionals. The U.S. government, therefore, must confront the cyber defense challenge as it confronts other military challenges: with focus not on numbers but on superior technology and productivity.

William J. Lynn, III, *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Aff. (Sept./Oct. 2010), *available at* http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Assigning DoD as the single agency responsible for this work and then adequately funding both personnel and research is a vital step in the right direction.

Conclusion

The threat from cyber attacks is certainly among the most important issues for American national security. The changing nature of the threat, the enemy, and the targets make this an issue of urgent and enduring importance. President Obama must focus the full attention and powers of the government on this issue to ensure the safety of the nation. Two important steps that will do much to accomplish this task are the overhaul of the current public-private partnership that he has made a key building block of his cyber strategy and the reallocation of the primary governmental responsibility for cyber security from the Department of Homeland Security to the Department of Defense. The U.S. can either act now with commitment and foresight or wait to do so in the aftermath of a potentially catastrophic cyber attack. ❍

[3] See id.

[4] See http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf.

[5] See http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war (requires registration).