The United States Is Not Ready for a Cyber Attack[i]

As the growth in the capability and sophistication of cyber bad actors continues to threaten national and economic security in the United States, confusion reigns and a lack of clarity exists as to who is in charge and how to deal with a significant cyber event that could become an incident of national or even global consequence.[ii] Cyber attacks increasingly target the U.S. military and other federal departments, causing these agencies to rely on technology to accomplish their goals, which also increases the size of their attack surface.[iii]

- The United States faces security challenges posed by near-peer nations such as China and Russia, which easily could cripple the nation's critical infrastructure with devastating results.[iv] Not far behind with increasingly sophisticated attacks are Iran, North Korea and global terrorist groups such as the Islamic State of Iraq and the Levant (ISIL) and al-Qaida. [v]
- The most dangerous threat to the United States may come from cyberspace rather than terrorists, according to a panel of experts.[vi] A cyberspace attack could wreak damage that would change the nature of the country, they suggested. [vii]
- The Internet of Things that will connect virtually all electronic devices in a surge of ubiquitous networking will be a target-rich environment to terrorists, saboteurs, criminals and other cybermarauders, according to a panel focusing on that aspect of future cyberspace.[viii]

The U.S. government has no cohesive or detailed retaliatory response to the increasing number of cyber attacks against national interests and security, a shortcoming that top U.S. intelligence leaders said disrupts the development of a deterrence framework.[ix] Unlike the dominance the U.S. military enjoyed for years in the conventional warfare realm, the lack of physical and geographic boundaries in cyberspace test modern warfighting doctrine.[x]

- No strategic blueprint provides high level direction, nor do any operational plans articulate roles and responsibilities for government, industry and other stakeholders during various thresholds of escalation throughout a significant cyber event.[xi]
- The United States does not have an approved national cyber incident response plan that provides documented, predictable and sustainable procedures and protocols for addressing what is characterized as one of the most serious threats facing the safety and security of our nation.[xii]

The formula for success in addressing the growing cybersecurity challenge in the United States and around the world includes a truly joint, integrated public/private operational capability fueled by information sharing, analysis and collaboration.[xiii] This will improve detection, prevention, mitigation and response to cyber events that may have national or even global consequences. [xiv]

- Throughout the United States—and in countries around the world—public, private, academic and non-profit organizations of all sizes are advancing education and awareness efforts to raise the consciousness for citizens in regards to cybersecurity.[xv] These collective efforts to raise the bar of cybersecurity protection, preparedness and resilience will help make the nation safer and more secure. [xvi]

- Officials want to strengthen partnerships between the government and industry and "find the right balance to enable the intelligence community and law enforcement to operate while still respecting the rights to privacy."[xvii]

Alternative Analysis

Countering a Cyber-Attack with Technology Is Not the Only Retaliation That Should Be Considered[xviii]

While an eye-for-an-eye approach may sound tempting, a cyber-response is not necessarily the best solution.[xix] Senior leaders will take a look on a case-by-case basis and determine the best capabilities for a U.S. government response. [xx] A cyber event is not necessarily different than a physical event in terms of when there's a threat to national security and what mechanism would be best to respond with. [xxi]

- NATO does not yet have a policy—let alone a definition—of what constitutes a cyber-attack that would mandate a response under Article 5 of the alliance's Washington Treaty, according to NATO officials.[xxii] Article 5 defines an attack on a NATO member as "an attack on all," requiring a response by all members against an aggressor. [xxiii]
- The U.S. government must continue to develop and refine its national cyber policy framework, which includes the evolution of all dimensions of a deterrence posture, and build up the "ability to deny the adversary its objectives, to impose costs and to ensure we have a resilient infrastructure to execute a multi-domain mission." [xxiv]

[i] 15862 United States Not Ready Cyber Attack
[ii] 15669 When Will United States Have National Cyber Incident Response Plan
[iii] 15661 Visibility Critical Enhancing Cybersecurity
[iv] 17069 US Intelligence Chiefs Testify Cyberthreats Nation
[v] 17069 US Intelligence Chiefs Testify Cyberthreats Nation
[vi] 13882 Cyber Overtakes Terrorism Main National Threat
[vii] 13882 Cyber Overtakes Terrorism Main National Threat
[viii] 13493 Internet Things Will Be Fertile Ground Cybermarauders
[ix] 17069 US Intelligence Chiefs Testify Cyberthreats Nation
[x] 17219 Information Warfare What It
[xi] 15669 When Will United States Have National Cyber Incident Response Plan
[xii] 15669 When Will United States Have National Cyber Incident Response Plan
[xiii] 16069 Situational Awareness Will Inform Risk Management Decision Making
[xiv] 16069 Situational Awareness Will Inform Risk Management Decision Making
[xv] 15415 Improving Cybersecurity Requires Teamwork and Collaboration
[xvi] 15415 Improving Cybersecurity Requires Teamwork and Collaboration
[xvii] 17069 US Intelligence Chiefs Testify Cyberthreats Nation
[xviii] 17069 US Intelligence Chiefs Testify Cyberthreats Nation
[xix] 15862 Cyber Not Always Answer
[xx] 15862 Cyber Not Always Answer
[xxi] 15862 Cyber Not Always Answer
[xxii] 13064 Nato Has No Article 5 Guidelines Cyber
[xxiii] 13064 Nato Has No Article 5 Guidelines Cyber
[xxiv] 17069 US Intelligence Chiefs Testify Cyberthreats Nation