Combating the Invisible Threat: Defensive Solutions for the Cyber Age

SCUSA 69 Policy Paper

Members: Carly Eckstrom, Justin Gittemeier, Sawyer Johnson, Adam Kaplan, Parker Lambes, Elaine Lee, Doha Sabbagh, Emily Snyder, Alex Werden, Jamie Withorne, Illina Yang, Brett Yelverton

Executive Summary

Our greatest cyber vulnerability is our critical infrastructure. While the threshold for offensive action against a cyber attack remains nebulous, defensive measures are within easy reach. By mandating best practices and promoting good cyber hygiene in private industry, the United States can protect its societal resources to avoid the need to act offensively against the forgotten, aggrieved, or weaker parties which can leverage cyber weapons' low barriers to access to their advantage.

Background

Critical infrastructure, according to the Department of Homeland Security, provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. Overall, there are sixteen critical infrastructure sectors that compose the physical or virtual assets which are so vital to the United States that their incapacitation or destruction would have a debilitating effect on national security, finances, public health, or safety (U.S. Department of Homeland Security 2017). A multi-pronged approach that leverages internal inducements and international collaboration can increase the resilience of critical infrastructure.

Critical infrastructure is a strategic target for cyber attacks. These cyber attacks may not cause loss of life, but will always cause loss of capability. Actors fight for a voice on the world stage by denying, disrupting (making a weakness in a system that is recoverable), and destroying (damaging beyond repair) systems. In 2015, Russia conducted a successful cyber attack that disrupted the northern Ukranian power grid for over four hours (Greenberg 2017). Chinese-linked cyber group Deep Panda conducted network exploitation against health care company Anthem, resulting in the loss of eighty million patients' healthcare records (Krebs On Security 2015). As an example of a kinetic attack, a state actor caused substantial damage to Iranian centrifuges through the use of the Stuxnet worm, detracting from their nuclear enrichment capabilities (Zetter 2014). Similarly, a Russian hacking group, Energetic Bear, targeted the United States' nuclear power plants in July 2017 (Porter 2017). Our policy recommendations focus on cyber attacks above the level of computer network exploitation like the ones mentioned previously.

Analysis

Cyber is the weapon of the weak because it provides access to large-scale disruption and destruction through avenues that would otherwise not be available to state and non-state actors with fewer resources. Cyberspace is a level playing field compared to the physical world we live in today. This policy paper analyzes cyber issues in the context of state and non-state actors and recommends development of domestic defensive capabilities to counter the asymmetrical tactics used by the forgotten and aggrieved.

State actors demonstrate their cyber capabilities in order to communicate their desire to rise within and challenge the liberal world order led by the United States and its close allies. While international law nominally governs the use of cyber capabilities, the lack of corresponding international

[1] We would like to thank Prof. Jennifer McArdle and LTC Tanya Estes for their professional expertise and mentorship in the creation of this paper for SCUSA 69.

norms, along with the difficulty of conclusively attributing cyber attacks to specific states, creates a gray area in which nations may violate cyber sovereignty without risking immediate kinetic retribution. States may also sponsor attacks by non-state groups to further complicate attribution, limiting the rhetorical space for victim states to urge kinetic retaliation. Revisionist states adversarial to the United States, including China, Russia, Iran, and North Korea, have used cyber attacks to demonstrate superiority, to maintain or establish regional standing, and to attempt to demonstrate parity with great powers.

Weak, non-state actors use the low costs of attack, political cover provided by massive data, challenges of attribution, control of scale, variable duration of attack, speed of recruitment, and geographic dispersion to gain leverage over stronger actors. These groups, such as Anonymous, cyber caliphate, and Petya/NotPetya, demonstrate the ability of the forgotten and aggrieved to voice their opinions and disrupt the world order. The capacity of these potential adversaries to carry out cyber attacks on the United States is a strong motivator to solidify and deploy a domestic strategy based on the fundamentals of cyber defense.

Cyber Defense Recommendations

1. *Compartmentalization of Systems and Data:* The United States' critical infrastructure systems and data should be compartmentalized with the intent to prevent large disseminations of critical information and cascading effects. While a compartmentalized structure may reduce efficiency, it mitigates risks of cross-system failures if a cyber attack were to occur. While government systems can be divided, private corporations in control of critical systems must be provided with incentives, such as tax breaks, to justify losses in efficiency.
2. *Enforcing Security in Critical Infrastructure:* The Department of Homeland Security will use the NIST Cybersecurity Framework to analyze the ability of private corporations to identify, protect, detect, respond, and recover, as well as implement good cyber hygiene (as outlined in Senate Bill 1475 and House Resolution 3010).
    a. If these critical infrastructure corporations, especially those with substantial quantities of personally identifiable information, are not identified to operate at Tier 4 on the NIST by a specific deadline they will be sanctioned. Less critical companies within the infrastructure realm can be incentivized by the government to adhere to the same Tier 4 standard by means of tax breaks.
    b. In order to facilitate the transition to a graded system within the given time period, the government will provide a red-team penetration test followed by the opportunity for risk analysts to quantify the effects of vulnerabilities on future operations. These tools and conclusions should be available within Information Sharing and Analysis Organizations.
3. *Improving Education:* DHS will provide training programs to increase public knowledge of cyber threats and common weaknesses. This training will be offered to employees of critical infrastructure companies and incentivized to increase participation.
4. *Applying counter-terrorism strategies to cyberspace*: Counter-terrorism strategy is predicated on an understanding of adversary motives before tailoring a response. A similar strategy could be applied in cyberspace, where the adversary rationale will be integral to determining appropriate defensive measures.
5. *International Cooperation:* Partnering with governments of non-state actors' host countries under Mutual Legal Assistance Treaties would address accountability measures on a transnational scale through prosecution of cyber attackers, and cross-industry partnerships would increase certainty of online behavior, as would empowering INTERPOL cybercrime fighting capacity through increased funding.

Works Cited

Greenberg, Andy. "'Crash Override': The Malware That Took Down a Power Grid." WIRED. Last modified June 12, 2017. https://www.wired.com/story/crash-override-malware/.

International Group of Experts. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, edited by Michael N. Schmitt. Cambridge University Press. 2017.

Krebs, Brian. "China To Blame in Anthem Hack?" *KrebsonSecurity*. Last modified February 6th, 2015. https://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

Porter, Tom. "All the Evidence Points to Russia in a Recent Hack of U.S. Nuclear Power Plants." Newsweek. Last modified July 7, 2017. http://www.newsweek.com/russia-russian-hackers-nuclear-power-633160.

Schneider, Jacquelyn. "Cyber Attacks on Critical Infrastructure: Insights from War Gaming." War on the Rocks. Last modified July 26, 2017. https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/.

U.S. Department of Homeland Security. "What is Critical Infrastructure." *Homeland Security*. July 12, 2017. Accessed November 3, 2017. https://www.dhs.gov/what-critical-infrastructure.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." WIRED. Last modified November 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.