Unifying U.S. Cyber Response

By Jacob Williams

Jacob Williams is a Masters of International Affairs candidate at the Bush School of Government and Public Service where he focuses on Cyber Policy, he will graduate in May 2022. He also serves as the Chair of the 66th Annual Student Conference on National Affairs, which provides programs on topics including national security, domestic policy, and international affairs.

Technology has revolutionized the way that the world interacts in every sphere, from social and economic interactions to election politics and nation-state competition. While this innovation has brought technology into the public sphere of policy debates, these debates often do not emphasize remaining secure through these innovations. Ignoring the security challenges associated with technological innovation or continuing without concentrated efforts to secure cyberspace will deeply damage U.S. national security. With awareness of these challenges, United States national security strategy must account for cyber threats or it will be unable to secure its interests both at home and abroad.

In the twenty-first century, the world has seen large trends of pervasive and destructive cyber intrusions, from economic espionage and financial attacks to kinetic cyberwarfare. According to a 2019 report by the IT solutions firm Radware "respondents indicated a substantial increase in the percentage of cyberattacks attributed to cyberwar," up from 19% to 27% in just one year.[1] These attacks, which can be traced back to several nation-state actors, display a concerning trend in the world of cyber conflict. The primary cyber adversaries to the U.S. and its allies have been Russia and China, with Iran and North Korea comprising a second tier of threat actors.[2] These adversaries have a diverse range of motivations for action including economic espionage, financial gain, political coercion and covert action. As a note, "hacktivism" and financial intrusions by non-state actors are also on the rise but are outside of the scope of this assessment.[3]

In this face of these rising intrusions, some in the public sphere have loudly sounded the alarm, warning of the next 'Pearl Harbor' being a cyberattack.[4] Recent cyber incidents have shown that our rivals are willing to utilize cyber capabilities in an adversarial manner, including Russian and Iranian critical infrastructure attacks, Chinese cyber-espionage, and Russian disinformation campaigns. With these capabilities being displayed across the international system, some observers have shown a concern that

[1] *Global Application & Network Security Report | Radware*. pp. 15. Retrieved July 15, 2020, from https://www.radware.com/ert-report-2020/

[2] *Crowdstrike 2020 Global Threat Report*. *CrowdStrike*, 7–9. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeGlobalThreatReport.pdf

[3] When discussing cyberwarfare, it is important to frame the conversation in an understandable and defined manner. For the sake of this work, I will be discussing instances of nation-state sponsored intrusions against critical infrastructure or communications technology. These actions can be motivated by several reasons, but all threaten the stability and security of the U.S. national security community.

[4] Stone, A. (2019, July 30). *How Leon Panetta's 'Cyber Pearl Harbor' warning shaped Cyber Command*. Fifth Domain. https://www.fifthdomain.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command/

the U.S. could be falling behind in the cyber arms race. In order to resolve this challenge, the U.S. must adapt to this new and constantly changing domain of warfare.[5]

This new domain of warfare presents several challenges that are unique when compared to other national security challenges including defending large and at-times antiquated networks, a wide distribution of defensive responsibilities, and the difficulty of attacker attribution. Firstly, the challenge of network defense is unique in warfare as it allows a threat actor to attack a much wider perimeter, as networks are spread throughout cyberspace. Secondly, U.S. cyber defense is spread between the Department of Defense, responsible for .mil domains, and the Department of Homeland Security, responsible for .gov domains and certain critical infrastructures. Finally, it is often difficult to pinpoint the identity of attackers and when that is possible, attacks often occur across national borders. With these pressing challenges, it is important to contextualize the cyber threat.

While much has been reported about U.S. vulnerabilities in cyberspace, many have ignored the important progress made by the U.S. in the offensive cyber domain. Beginning in 2010, it was discovered that a joint U.S.-Israeli cyberwarfare program had resulted in the first "cyber-physical weapon technology".[6] This digital weapon, known as Stuxnet, wreaked havoc on Iranian nuclear centrifuges and displayed arguably the most sophisticated digital attack in history. With this attack tying back to U.S. military and intelligence organizations services, it shows U.S. offensive cyber capabilities as much more advanced than generally regarded, but possibly less willing to utilize these capabilities than other near-peer adversaries.

As our adversaries continue to push the boundaries of cyber conflict with relative impunity, it is crucial that the United States unifies its response against these persistent threat actors. Currently, cyber defense is largely divided between DHS and DOD, with each organization responsible for separate networks and separate domains, with the DOD handling military operations and the DHS responsible for critical infrastructure. Unfortunately, cyber conflict cannot be relegated to either of these domains, with a high possibility of intrusions that transcend the borders of these organizations' networks. The complicated nature of the cyber domain has even led to debate over whether to create a standalone cyber force, argued prominently by ADM James Stavridis, who is the former Supreme Allied Commander Europe and former Dean of the Fletcher School of Law and Diplomacy.[7] While this proposal has a number of challenges of its own, it is also practically unlikely with U.S. Space Force still in its infancy.

One step in unifying the response to cyber conflict is increasing the representation of cyber affairs at the policy-making level. For example, in the public sector, leadership in cybersecurity is almost always subordinated to leaders who must balance these issues against threats such as terrorism, physical infrastructure security, or combat operations. As a result, cyber issues will not receive the necessary amount of recognition, despite their vast importance to national security. To resolve this issue, it is

[5] *America is losing the cyber war*. (2018, May 11). Security Info Watch. https://www.securityinfowatch.com/cybersecurity/information-security/article/12412249/america-is-losing-the-cyber-war

[6] To Kill a Centrifuge | Detailed Stuxnet Analysis | Langner. (n.d.). Retrieved July 14, 2020, from OT/ICS Asset Management | Langner website: https://www.langner.com/to-kill-a-centrifuge/

[7] Stavridis, James and David Weinstein. Time for a U.S. Cyber Force. (2014, January 1). U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2014/january/time-us-cyber-force

important to solidify consistent representation for cyber-specific issues at levels including the National Security Council, the Joint Chiefs, and in Congress. One method to do this is through a designated coordinator for cybersecurity, like the position held by Rob Joyce until 2018. Successful coordination of cybersecurity efforts within the White House could create an important emphasis on joint efforts, better unifying the U.S. response to cyber issues.

One final avenue in confronting rising cyber intrusions is creating stiffer penalties for malicious actions and utilizing cyber capabilities to respond to persistent threats. As discussed above, U.S. offensive capabilities are likely cutting edge and have been used as a deterrent against threat actors. While there are several challenges with responding to nation-states within cyberspace, exploring these capabilities could give decision-makers a wider range of options between financial sanctions and combat operations. While it is imperative that the U.S. creates policies that account for proportionate responses in the face of cyber intrusions, the options created could further strengthen U.S. national security.

Many threat actors have persistently tested the limits of U.S. cybersecurity, without facing strong repercussions. In order to adapt to this ever-changing domain, the national response must be unified and utilize resources available throughout the federal government in order to defend the country against these threat actors. While the U.S. is not facing the possibility of overwhelming cyber-conflict at this moment, we must prepare for a day when this could be a reality.