Assessing US Cyber Security Policy Against Major Peer Competitors

Brett Biscoll

Johns Hopkins University

Military Strategy and National Policy

Professor Michael Noonan

December 10, 2023

Introduction

Despite ongoing debates about the nature and trajectory of cybersecurity's role in military strategy, the substantial resources allocated by major state-level actors and the heightened interest it garners within the security community justify a closer examination of the approach taken by the United States. However, this must be done with the knowledge that cyberwarfare is a new domain, characterized by a greater potential for deception than ground, naval or air operations. This is a result of the innate difficulty of perceiving a cyber attack, which often does not come with a physical presence of any sort; furthermore, it is often difficult to trace attacks of this nature to their source. Due to these factors, it is difficult to pinpoint all the benefits and drawbacks of the current cyber security policy merely by taking public statements at face value; instead, one needs to take an in-depth look into both what has been made public regarding the known and suspected cyber operations of the United States, and what the resulting impact is on the behavior of major competitors. By taking this in-depth look, we can form a partial but informed answer to the question of how effective the United States' approach to cyber security has been in accomplishing national security goals.

Literature review

The theoretical landscape surrounding cyber security is defined by its relative novelty in the field of military policy. In *Modern Military Strategy*, it is noted that "Strategic thought on cyberwar is in its infancy" (Sloan, 141). What this signifies is that unlike other domains of warfare, which can draw from decades of theories and are informed by a plethora of historical cases, cyber security has a much more limited history to draw upon, and many common theories are in need of more real world evidence to confirm. Moreover, our ability to scrutinize real,

historical scenarios of cyber defense is further constrained by the fact that "...Information is admittedly sparse, in part because strategic thought on cyberwar is relatively new, but also because the combination of military organizations as strategic thinkers, and the close link between cyberwar and intelligence assets, means that only limited information exists in the unclassified domain" (Sloan, 141). In other words, what we have available is only a portion of what truly exists. However, this should not be understood to mean that it is impossible to make a meaningful analysis of the cyber security landscape; instead, the secrecy should be understood as an active element in the existing cyber strategy.

Our understanding of the cyber security landscape and the United States' policy within it can be developed by reviewing what theories have been published surrounding the domain. The most fundamental part of developing an overarching theory of cyber security is to define what the term 'cyber security' itself means. Several competing definitions exist; on one end of the spectrum is a strict definition used by Herbert Lin in his article 'Offensive Cyber Operations and the Use of Force': that is, "'the use of deliberate actions – perhaps over an extended period of time – to alter, disrupt, deceive, degrade or destroy adversary computer systems or networks and/or programs resident in or transiting these systems or networks'. " (Lin, 63) On the other end of the spectrum, we have an expansive definition used in the article 'Cyberwar is coming!', which states that "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles.…disrupting, if not destroying, information and communications systems…It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, …It means using knowledge so that less capital and labor may have to be expended." (Arquella and Ronfeldt, 146).

The opposing views described here are evidence to the fact that a consensus has not yet developed with regards to an exhaustive list of what exact operations fall under the banner of cyber security; one example of an action on this as yet undefined border is that of psychological operations (PSYOPs), often considered part of cyber warfare due to the focus on information (and misinformation); however, a psychological operation can conceivably be done without using any technology more complex than leaflets and posters; low-tech tactics like this are not usually considered part of cybersecurity, hence the controversy. Another example of an activity on the border of cyber and non-cyber warfare would be electronic warfare - that is, anything weaponizing the electromagnetic spectrum. Electronic warfare has a long history, stretching as far back as signal jamming operations in the Russo-Japanese War. The extent to which these borderline cases fall under the cyber domain depends on the theorist in question and the definition in their respective doctrine.

In addition to scope, the contemporary approach to cybersecurity and the arguments around it have disagreed on whether it should be used as a defensive or offensive measure; the conversation has trended from the former to the latter over time in the United States. Initially the domain was conceived strategically as consisting mostly of operations which were "implicitly and invariably centered on…computer strikes against computer systems." (Sloan, 143).” However, this policy was quickly changed to include an offensive component when "In 1998 the Pentagon established the Joint Task Force – Computer Network Defense with a mandate to protect the Pentagon’s computer networks, and in 2000 the Task Force was also assigned an offensive mission." The shift from NATO on “computer network defense” was likely to have developed as a response to competitors; Russia has leveraged offensive cyber capabilities, and China has openly discussed the benefits of such operations.

A last point on the theory that informs the cyber policy is the uniqueness of the landscape cyber operations occur in. Unlike other forms of warfare, there is not one single definable cyber expanse to be conquered and controlled; rather, it is amorphous and "only useful as a form of warfare against entities with fairly extensive computer networks" (Sloan, 147), with the potential to wreak widespread damage in a single attack. Additionally, it is worthwhile to note that permanent, repeatable damage may not be feasible in the cyber domain, as a successful attack reveals vulnerabilities that can then be patched; the goal is to coerce, assert status, disable or support other elements in one operation.

Thesis & Hypothesis

With this foundational knowledge of the cyber domain, we can now look into the officially articulated strategy on cyber security. The most obvious way to understand the United States' approach to this domain is to go to the *2023 Department of Defense Cyber Strategy Summary.* This document highlights that American prosperity and security "depends upon a free, open, and secure cyberspace"; and highlights the importance of information technology in the United States domestically and implies the potentially catastrophic danger posed by a cyberattack. The Department of Defense then identifies main competitors of concern with respect to cyber, most prominently calling out Russia, Iran and the People's Republic of China, all charged with "embrac[ing] malicious cyber activity as a means to counter U.S. conventional military power and degrade the combat capability of the Joint Force". Other competitors are mentioned, including North Korea and various extremist organizations; however, due to the earlier mentioned emphasis on "entities with fairly extensive computer networks", China, Russia and Iran make up the majority of the focus.

The actions the Department highlights to achieve success in the cyber domain include "four complementary lines" (DoD, 2022) covering a a focus to 'Defend the Nation', by conducting active attacks against malicious actors, a tactic that relates to the growth of offensive capabilities as part of cyber security; to 'Prepare to Fight', by enhancing the Joint Forces' ability to fight in cyberspace by leveraging the original defensive component as well as making a point to "utilize the unique characteristics of cyberspace" which make it unlike other domains; to 'Protect the Cyber Domain with Allies' by promoting jointness with international partners and enforcing 'internationally recognized cyberspace norms', and to 'Build Enduring Advantages' by focusing on education and institutional reform to stay competitive in a dynamic area. In short, the strategy is to defend, prepare, protect, and build the cyber capabilities of the United States.

With these four lines of effort informed by the major theoretical arguments around cybersecurity, we have a baseline for how to analyze the United States' cybersecurity strategy. When we review the major cases of cyber security in recent history as it pertains to major competitors to the United States, we find that the approach to cyber defense has been effective in promoting American security.

Methods description

For my analysis, I will focus on leveraging the method of concomitant variation by analyzing how the US efforts to defend, prepare, protect, and build out cyber capabilities result in a proportional reduction in the scale, frequency and effectiveness in cyber attacks from other competitors, as well as produce results in support of other domains of warfare. The variables I analyze are qualitative in nature, but will follow the following pattern of identifying what the competitors to the United States are doing, what the United States' response as informed by the

principles laid out in the cyber defense strategy has been, and what the resulting change in the behavior of our competitors is.

Evidence

The competitors I will analyze will be the three largest as noted in the cyber defense strategy - those being Russia, Iran and China. Russia is perhaps the most prominent of these, as they present an active threat to the United States and allies in the land domain through the ongoing war in Ukraine. At the outset, the conflict was expected by observers to have a large cyber component (CSIS, 2023). However, this did not play out quite as expected: "Yet, Russia has not launched an all-out, costly cyberwar against Ukraine or its backers in the West. The so-called “thunder run” never materialized." There has been “a Russian preference for waging a global campaign focused more on misinformation and undermining support for Kyiv” rather than an intensification of cyber assaults targeting infrastructure. While attacks did occur, “the empirical evidence demonstrates that while there has been an uptick in cyberattacks… these attacks did not demonstrate an increase in severity, a shift in targets, or a shift in methods.” Ultimately, the cyber offensive from Russia comes off as relatively weak compared to expectations; as analyzed by the Center for Strategic and International Studies, “On a scale from 0 to 10, with “0” representing no cyber activity and “10” representing massive death as a direct result of a cyber incident, Russia’s attacks targeting Ukraine never surpassed a “5”—single or multiple critical network infiltrations and attempted physical destruction,” (CSIS, 2023).

While Ukraine is of course the main target of Russia’s attacks relating to the ongoing conflict, Ukraine, the United States and other allies can be understood here as a members of a combined front opposing Russia, especially in the context of significant, preexisting, public

support in recovery of cyber attacks, with an NSC spokesman saying that “We [the US] will provide Ukraine with whatever support it needs to recover," (Webber). Additionally, President Biden has explicitly mentioned that the United States was ”Working closely with …the private sector to harden their [Ukraine’s] cyber defenses, sharpen our ability to respond to Russian cyberattacks as well” (The White House).

The showing of substantial support from the US puts the unexpectedly soft cyber attack from Russia in a new light. It would not be the first time that Russia and the United States have engaged each other in cyber operations, either directly or by proxy. Suspected Russian cyber attacks include 2020 US government data breach and the DarkSite ransomware event. The former resulted in large data theft and significant costs in rescuing government systems, while the latter impacted much of the Colonial Pipeline. On the other side, the US is suspected of performing an attack on the Russian electrical grid (BBC), with a claim from The Times who said that “...this was an escalation of other work the US was doing to combat Russian disinformation and hacking campaigns.” Due to the concealed nature of these attacks, it is hard to deduce exactly what extent of the limited Russian response can be attributed to Ukrainian defenses, the threat of US retaliation, or some additional third factor (such as a lack of preparation on the Russian side). While the United States' policy did not fully deter Russia from attacking Ukraine and US systems, it did seem to limit the severity of attacks, and as a result the US was able to engage in offensive engagements and operate in a contested space by hacking Russian infrastructure. From the perspective of the cyberspace objectives as laid out by the Department of Defense, these were clear successes in defending, preparing and protecting US systems.

The next competitor identified in the Department of Defense's strategy is Iran. Similar to the approach taken by Russia, recent decades have seen a shift away from direct military engagement in the land, sea, or air domains; however, the distinctive clandestine nature of cyber warfare once again makes it a prime arena for both parties to engage in operations against each other.

Iranian sabotage efforts have been aggressive, having “gone beyond simple web defacements” (Newsweek) and included “destroyed data and shut down [of] access” to critical websites, notably in the 2014 attack against Las Vegas Sands Corporation and in “massive distributed denial-of-service attacks” against US banks around 2012-2013. For these reasons, the Iranian cyber warfare program is widely seen as a threat by the United States. However, the dynamic of cyber security between the US and Iran is not wholly of the US being on the defensive; while never officially confirmed, the STUXNET computer virus is widely suspected of being used by the United States against Iran, with observers citing two main points as evidence.

The first piece of evidence is that, unlike other viruses, “Stuxnet appears to target industrial control systems” and only activates in specific conditions (Chen, 2011*)*. The exact intended goal is unknown, but it was known to have infected between 50,000 to 100,000 computers, in “Iran (58 percent), Indonesia, India, and Azerbaijan," suggesting a targeted operation.

The second reason to believe STUXNET is attributable to the United States is the complexity of its code. It has a code size of 500 Kbytes and is in multiple languages, much bigger than similar viruses. Additionally curious is the use of , "...an unprecedented four

zero-day Windows exploits. Attackers value zero-day exploits, so four represents an unusually high investment" on the part of the creator- suggesting a creator with significant resources.

The virus is known to have impacted the Iranian nuclear program by damaging several centrifuges, a point that was confirmed by the president of Iran. However, it is worth nothing that the virus, impactful and complex as it was, was not a total blocker for the Iranian nuclear program; in *Stuxnet to Sunburst,* its damage was described as having "derailed and delayed" the program "only for several months," and that "Iran's capability and operation would increase, it certainly was not halted. More of a bloody nose than a knockout and a rather expensive one as it would ultimately prove." However, the limited nature of the STUXNET impact should not discount the evidence it shows of cyber impacting another domain of warfare.

From the perspective that cyber is a supporting element of warfare, focused on helping to achieve success in other domains, the STUXNET virus seems to be a qualified success in maintaining an edge. Both groups have launched cyber operations against the other, but the introduction of STUXNET to impact the Iranian nuclear program was not to be a deterrent against cyber attacks, but a cyber offensive to protect US interests by slowing down the Iranian nuclear program. Therefore, it should be seen as a proof of success in defending US interests with a forward operation, and leveraging the unique aspects of cyberspace to the strategic benefit of the United States.

The third major competitor of the United States' cybersecurity strategy is China. Similar to Russia and Iran, China maintains the common strategy of leveraging the cyber domain as an alternative to direct engagement in the ground, naval, or air domains, where the United States holds a strong advantage. One difference in the approaches of Russia and Iran in comparison to China is that generally is generally considered more aggressive in their use of cyber attacks.

Notable cases of China's interference include hacking into Microsoft's company servers (Guardian) and Google's networks. These were both done in spite of previous cybersecurity agreements that prohibit the theft of intellectual properties (Guardian). However, cyber attacks from China go further than the simple theft of intellectual property. In one instance particularly concerning to the United States, China was able to identify CIA personnel by using stolen data; "Undercover CIA personnel, flying into countries in Africa and Europe for sensitive work, were being rapidly and successfully identified by Chinese intelligence, according to three former U.S. officials" (Foreign Policy). This was done through what was suspected to be a "suave and professional utilization" of key personal and private informational datasets. While running into the usual attributability problem we encounter for cyber attacks, these events are evidence of a continuous cyber operation by China against the United States.

The cyber security measures taken by the United States in retaliation to China are mostly hidden as well; nevertheless, evidence reveals active engagement in counter-espionage operations within the cyber domain. Notably, this includes the breaching of Chinese servers (Forbes) and the hacking of mobile phone data, though this was only claimed by former NSA agent Edward Snowden. Further US actions against China follow a pattern of hacking key data for later use; a separate incident (CNBC) noted that a communications interception was used to penetrate their systems and access sensitive information- though what such information would be used for is, again, not publicly revealed.

China represents another situation where the characteristic covertness of the cyber domain makes establishing cause and effect somewhat difficult. What we can confirm is that China and the United States are active in cyber operations against each other involving gathering data for use in other domains. While the balance of attack between the two countries seems like a

mixed success at best, it is important to note that, as described in a report by Booz Allen, China is only hacking "below the threshold of war" (Booz Allen). This itself is a success in the cyber domain; that China feels compelled to limit the scale of their operations commensurate with the United States' ability to respond in kind represents a kind of strategic balance that keeps the cyber conflict within defined limits.

Findings

At the risk of overly repeating the point, it is essential to once again highlight that a significant portion of the information pertaining to the cyber domain is classified or undisclosed. Therefore, our examination provides only a partial glimpse into the historical operations the United States has conducted. Nevertheless, from the recent history of cyber defense with these three main competitors we see the common thread of how the US cyber defense policy - to defend, prepare, protect, and build- has resulted in meaningful benefits to the United States and its allies in the cyber domain and supported domains. For Russia, the threat of of the US to "sharpen our ability to respond to Russian cyberattacks" helped curb the severity of their cyber operations against US ally Ukraine; for Iran, the STUXNET virus helped to slow down the Iranian nuclear program, buying time to develop strategies to curb Iran in the future, and proving that cyber defense operations can be effective in producing a benefit in another domain. Lastly, for China, we see proof of cyber retaliation against their attacks in the form of breaching servers and mobile data for use in other intelligence related operations, all of which have helped to keep China's operations "below the threshold of war". For these reasons - limiting Russia and China's cyber offensives and damaging Iran's nuclear capabilities - the United States' approach to cyber security can be marked as a success.

The policy implications of this going forward will be dependent on how the cyber domain develops. As we continue towards what many expect to be a world increasingly impacted by technology and information, the stakes of having a solid cyber security policy will increase in equal measure, and drive further research on the part of malicious actors who seek military benefit and those who want to protect and secure their information. Therefore, the pursuit of more aggressive research into cyber operations to actively deter future attacks will be necessary if the United States wishes to continue protecting itself and its allies in the cyber sphere. The policy recommendations from that research will likewise evolve as time goes on, but should consist at the very least of more intense versions of what was described in this article: working with allies to provide protection, sabotage of systems used against the United States, and counter operations against data theft.

Finally, it is worth discussing what areas warrant future research on this matter. Perhaps the most pressing issue for the realm of cyber security is to get a full understanding of the past; as highlighted throughout the article, much of the information surrounding cyber operations remains classified or otherwise unknown. Uncovering more information behind the source and methods of unattributed cyber attacks and operations will help to provide a clearer and more accurate vision of the cyber landscape. Finally, the ongoing advancement of new technologies will keep the nature of the cyber domain in a state of flux, meaning that much of the operational information or the infrastructure behind cyber security is subject to change; creating a vision of the future technological landscape will be instrumental to developing a plan for cyber security for the next few decades and beyond.

Works Cited

Arquilla, John, and David Ronfeldt. "Cyberwar is coming!" *Comparative Strategy*, vol. 12, no. 2, 1993, pp. 141–165, https://doi.org/10.1080/01495939308402915.

Corporation. "China's Cyberattack Strategy Explained." *Booz Allen*, Booz Allen Hamilton, 16 Nov. 2022, www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html.

Denning, Dorothy. "Iran Is Now a Major Cyber Threat to the U.S." *Newsweek*, 12 Dec. 2017, www.newsweek.com/irans-cyber-warfare-program-now-major-threat-united-states-745427.

Dorfman, Zach. "China Used Stolen Data to Expose CIA Operatives in Africa and Europe." *Foreign Policy*, 1 Jan. 6796, web.archive.org/web/20201221112115/https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.

"Experts Say China's Low-Level Cyberwar Is Becoming Severe Threat." *The Guardian*, Guardian News and Media, 23 Sept. 2021, www.theguardian.com/world/2021/sep/23/experts-china-low-level-cyber-war-severe-threat.

Kharpal, Arjun. "China Alleges U.S. Spy Agency Hacked Key Infrastructure and Sent User Data Back to Headquarters." *CNBC*, CNBC, 27 Sept. 2022, www.cnbc.com/2022/09/27/china-alleges-us-nsa-hacked-infrastructure-sent-data-back-to-hq.html.

Lin, Herbert S. “Offensive Cyber Operations and the Use of Force.” *Journal of national security law & policy* 4.1 (2010): 63-. Print.

Mueller, Grace B., et al. “Cyber Operations during the Russo-Ukrainian War.” *CSIS*, www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Accessed 10 Dec. 2023.

National Research Council, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, DC: National Academies Press, 2009), 11

Rapoza, Kenneth. “U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press.” *Forbes*, Forbes Magazine, 22 June 2013, www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/?sh=3d7531f15340.

“Remarks by President Biden on Russia’s Unprovoked and Unjustified Attack on Ukraine.” *The White House*, The United States Government, 24 Feb. 2022, www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/24/remarks-by-president-biden-on-russias-unprovoked-and-unjustified-attack-on-ukraine/.

Sloan, Elinor C. “Chapter 8 - Cyberwar .” *Modern Military Strategy an Introduction*, Routledge, Taylor & Francis Group, London, 2017.

Stuxnet to Sunburst: 20 Years of Digital Exploitation and Cyber Warfare ..., www.amazon.com/Stuxnet-Sunburst-Digital-Exploitation-Warfare-ebook/dp/B09DT8YVFF. Accessed 10 Dec. 2023.

Summary 2023 Cyber Strategy of the Department of Defense.

T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," in *Computer*, vol. 44, no. 4, pp. 91-93, April 2011, doi: 10.1109/MC.2011.115.

"US and Russia Clash over Power Grid 'Hack Attacks.'" *BBC News*, BBC, 18 June 2019, www.bbc.com/news/technology-48675203.

Webber, Caitlin. "U.S. Offers Ukraine 'whatever Support It Needs' to Recover from Cyberattack." *Reuters*, Thomson Reuters, 14 Jan. 2022, www.reuters.com/world/europe/us-offers-ukraine-support-needed-recover-cyberattack-2022-01-14/.