HOOVER INSTITUTION

Summer Policy Boot Camp

2022 DIRECTOR'S AWARD WINNERS

Recalibrating Cyber Defense: Proposal for a Networked National Cyber Strategy

By Morten Hybschmann, political science student at the University of Copenhagen, sergeant in the Danish army, and student assistant in the Danish Ministry of Finance.

As societies, economies, and lives have become more digitalized, cyberattacks have become a central part of public discourse, policy making, and defense planning. Such attacks range from digitally enabled disinformation campaigns and distributed malware or ransomware to even an envisioned "Cyber Pearl Harbor." This essay argues that up until now, policy makers have misinterpreted the threat posed by cyber warfare. This has led to misaligned resources, insufficient preparedness, an out-of-sync ecosystem, and illusions about the offensive capabilities and ambitions of the United States and its adversaries. Thus, a change of policy in the Biden administration's upcoming strategy is recommended. A new policy should do two things: (1) decentralize cybersecurity measures into a network structure and (2) modify the United States' international stance to create a more credible deterrence and to support international norms. The goal is to ensure a correct understanding of the threat and an efficient use of taxpayer money while increasing the security of American citizens, companies, and institutions.

Three Strategies - Three (Mis)conceptions

The previous three presidential administrations have misunderstood the threat posed by cyberattacks. In the eleven years since the first national cyberspace strategy, technological advances have enhanced both protective and offensive measures available for the United States and its adversaries. However, the most fundamental change is the interpretation of the risks from cyberspace. Particularly, the three strategies have differed in their assessments of the likely devastation from a successful attack, how to best counteract such attacks, and the usefulness of cyber capabilities near or over the threshold of war.

President Obama entered the White House with a starry-eyed view of cyberspace. His administration's strategy from 2011 was inspired by the onset of the Arab spring and it saw cyberspace as a place "where the norms of responsible, just, and peaceful conduct amongst states and peoples have begun to take hold."[1] Vagueness and uncertainty also dominated the resulting strategy from the Department of Defense (DoD) in defining "cyber," especially with regards to how the DoD should react and organize in this new domain of warfare.[2]

In his second term, the Obama administration reassessed the risk, including from China and Russia, rearranged national coordination, and limited the range of operations possible by the DoD. Resilience and deterrence were built up through a variety of initiatives domestically.[3] The primary responsibility was given to the Department of Homeland Security, and the DoD was placed in a holding position

to avoid escalation, as the use of cyberattacks was considered on the threshold of war.[4] By the words of former US defense secretary Leon Panetta, the conception was that the United States was susceptible to a "cyber Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation."[5]

With the entry of the Trump administration, the gloves were off. The DoD changed its doctrine to a concept of "defend forward" and the cyber domain was presented as a constant competition rather than escalatory and existential.[6] However, the strategy of deterrence through strength did not stop new attacks, and early 2020 saw a distinct increase in serious cyberattacks on major companies and government agencies.[7] Likewise, on the offensive side, the forecasted success of cyber operations appears to have been significantly overstated. Consequently, it is clear that a reassessment is needed.

Reassessing Cyber Operations as a Weapon

After more than a decade since the first strategy, it's time to reassess both the research and real-world experiences. Policy makers should focus on three central points.

First and foremost, cyber operations are unlikely to escalate into armed conflict and are of limited effect in warfare. From recent confrontations between adversaries such as North Korea and South Korea, war games, and academic literature, evidence shows that cyber operations by state actors are very unlikely to provoke military action.[8] Instead, they are more often used as an alternative to such conflict as they are ambiguous, hard to attribute, and nonlethal.[9] Instead, cyber operations should be interpreted as a means of subversion, since they are "too slow, too weak, and too volatile to shift the balance of power in a targeted, predictable, and timely fashion."[10] Most recently, the war in Ukraine has shown how cyber operations have limited effect. Not even the feared cyber operations of Russia seem to have had a real strategic impact.[11]

However, this does not mean that the United States is not vulnerable to cyberattacks - especially in the form of disinformation and subversion campaigns, as well as malware and ransomware targeting the private sector. The economic costs alone from cyber crime are estimated to be in the range of 0.9–4.1 percent of GDP.[12] This astronomical number is set to increase even further due to remote work following the pandemic.[13]

Furthermore, cyber power, in comparison to military might, can be considered a "reverse structural power" where the most powerful actors are the most vulnerable.[14] A highly digitized society, an open system of government, and the supremacy of the biggest economy in the world give the United States a much greater potential for harm and turn its very strengths against it.[15]

Finally, while it is impossible to prevent cyberattacks, their impact can be constrained by building resilience. The decentralized and diffuse nature of cyberattacks makes their impact very hard to anticipate. This factor calls for resilience created not only

by investments in networks and infrastructure but also by increasing the human capital of the many digital users and citizens in general.[16]

Policy Recommendations for Biden's New Cyber Strategy

In the coming months, President Biden is expected to publish his new cyber strategy, which has been in the works since he entered office.[17] Based on the misconceptions of the previous strategies, and the evolved conception of the cyber threat, an effective strategy should encompass at least three overlooked elements: (1) decentralizing cybersecurity while maintaining federal crisis control, (2) reprioritizing funding from DoD, and (3) changing posture internationally.

Unlike other domains of modern war, the most efficient way to create deterrence and defense from cyberattacks is not by centralizing resources within a professional force—but instead by creating resilience in society from the bottom up. Many advances have been made by the current and previous administrations to bolster national interagency cooperation. And this is important, as their capabilities are crucial for coordination in times of crisis. However, Biden's new strategy is expected to aggressively expand the role of the federal government in cyber defense. [18] Instead of focusing on regulations and a hierarchical system that has led to "massive intelligence disconnects" and distrust between federal entities and the private sector, the new strategy should instead advance a network-based and decentralized cyber defense.[19]

A fundamental pillar of a networked approach to collaboration among federal, state, and local governments as well as the private sector is to bolster and multiply the regional centers under the Cybersecurity and Infrastructure Security Agency (CISA). This would entail a public-private partnership that, if done well, would overcome many of the vulnerabilities in the current cyber defense.

First, the regional centers' partnerships with academic institutions, private companies, and local governments could be catalysts for fixing the cybersecurity workforce gap with currently 2.72 million unfilled positions.[20] This could be done by linking early STEM education, professional cybersecurity training, and re-skilling of the workforce.

Second, the initiative would support the private sector in the difficulties it has faced when cooperating with the federal government in sharing information, knowing who to contact, and creating general trust. This would also support the smaller companies and state- or municipal-run utilities that frequently lack the funds and financial incentives necessary to adopt cybersecurity measures.[21] Regional offices, and the closer cooperation they allow, are particularly valuable in disaster planning and urgent response after an attack. The current cybersecurity infrastructure focuses overwhelmingly on the "left of boom," that is, staving off attacks by raising the collective level of security and implementing cybersecurity standards through regulations.[22] But disasters will happen, and thus we also need a focus on mitigating the disaster's effect in the aftermath, "right of boom."[23] Building regional offices would be effective for this, since there is the right concentration of business, critical

infrastructure, and knowledge of the overall risk landscape.[24] Existing examples from Australia and Texas verify that this is a functional and efficient organization of resources that provides local benefits and national security.[25]

Finally, successful implementation will require personnel, reorganizations, and funding. However, the latter might correct the misalignment of resources that has dominated US cybersecurity efforts. The DoD, which is primarily in charge of external cyber operations, has for fiscal year 2023 requested nearly $58 billion in IT and cyberspace funding, while CISA, the agency in charge of domestic cybersecurity, is set to receive $2.9 billion.[26] While this is a needed dramatic increase in both agencies' cyber funding, it signifies an ill-advised prioritization of funds that is harmful to not only taxpayers' wallets but to the security of American citizens, institutions, and companies. The misalignment stems from the illusion of a "cyber Pearl Harbor" and the misconception that cyber operations will be the new deciding frontier in warfare. It is, however, not optimal when facing a diffuse threat that rarely harms people (physically) and must be handled at a decentralized level.

International Change of Posture

The aforementioned domestic changes, while they may be the most effective, cannot stand alone in a new strategy. Internationally, the United States should change its posture on two dimensions to reduce the severity and frequency of cyber activities, mainly by adversaries such as Russia, China, and Iran. A primary task is reducing the strategic ambiguity left over from previous strategies by declaring to rivals (and allies) what is off limits and then deterring these strategic cyberattacks by threatening retaliation.[27] If everything is declared as critical infrastructure—and worthy of up to nuclear retaliation—then the notion itself loses credibility and the deterrence fails to work.[28]

Additionally, the Biden administration should continue its work creating (and respecting) norms for cyberspace in the international system. The White House has issued a common declaration with more than sixty countries, calling for "an open, free, global, interoperable, reliable and secure Internet" in contrast to the rising tides of "digital authoritarianism."[29] However, statements are not enough, and the United States should put force behind the words by adopting a no-first-use policy of strategic cyberattacks, including that the it will refrain from attacking, for example, civilian infrastructure preemptively, to build trustable norms and international law in cyberspace.[30]

Evaluation and Conclusion

The overall effectiveness of this proposed policy should be measured by (1) the number of regional hubs established under CISA, and the frequency of their engagements with regional companies and institutions, (2) an increase in citizens, companies, and agencies trust in cybersecurity measures, (3) the closing of the cyber workforce gap, and (4), most importantly, a reduction in the number of successful cyberattacks against the United States, their severity, and the total time of response to any identified attack.

Cyberattacks have already reached a degree and severity that constitute a crisis under the Biden administration.[31] The upcoming strategy has the chance to reconfigure and reinforce this crucial part of national security. Instead of continuing on his predecessors' path of centralization and offense, Biden should instead opt for a decentralized, networked approach. In the words of Lt. General Stanley McChrystal, "it takes a network to defeat a network."[32]

References

Edgar, Timothy H. 2022a. "A Year of Hacks and Cyberwar: How Biden Is Tackling Cybersecurity." The National Interest, April 18. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/year-hacks-and-cyberwar-how-biden.

———. 2022b. "Biden's Positive Cyber Strategy: Optimism Tempered by Experience." The National Interest, May 7. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/biden%E2%80%99s-positive-cyber-strategy.

Executive Office of the President of the United States. 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." CreateSpace. https://doi.org/10.1037/e688502011-001.

Kennis, Graham, and Lauren Zabierek. 2022. "Building a Regional, Right of Boom Cyber Defense Network." War on the Rocks, June 7. https://warontherocks.com/2022/06/building-a-regional-right-of-boom-cyber-defense-network.

Lonergan, Erica D. 2022. "The Cyber-Escalation Fallacy." Foreign Affairs, April 15. https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy.

Maschmeyer, Lennart. 2021. "Why Cyber War Is Subversive, and How That Limits Its Strategic Value." War on the Rocks, November 17. https://warontherocks.com/2021/11/why-cyber-war-is-subversive-and-how-that-limits-its-strategic-value.

———. 2022. "Subversion, Cyber Operations, and Reverse Structural Power in World Politics." European Journal of International Relations, August. https://doi.org/10.1177/13540661221117051.

McChrystal, Stanley. 2011. "It Takes a Network." Foreign Policy, February 21. https://foreignpolicy.com/2011/02/21/it-takes-a-network.

Minárik, Tomáš. 2016. "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit." NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit.

Ratnam, Gopal. 2022. "House Budget to Provide $15.6 Billion for Cybersecurity." CPA Practice Advisor, July 12. https://www.cpapracticeadvisor.com/2022/07/12/house-budget-to-provide-15-6-billion-for-cybersecurity/55147.

Reilly, Briana. 2022. "DOD Wants to See 2.5% Increase in IT, Cyber Funding in FY-23." Inside Defense, June 7. https://insidedefense.com/insider/dod-wants-see-25-increase-it-cyber-funding-fy-23.

Rivero, Nicolas. 2021. "Stop Waiting for a 'Cyber Pearl Harbor.'" Quartz, August 10. https://qz.com/2044945/the-threat-of-a-cyber-pearl-harbor-is-a-red-herring.

Schneider, Jacquelyn. 2022. "U.S. Military Strategy and Domestic Coordination." Testimony before the United States-China Economic and Security Review Commission.

Security Magazine. 2022. "Texas Launches Regional SOC for Local Cybersecurity Support," April 20. https://www.securitymagazine.com/articles/97462-texas-launches-regional-soc-for-local-cybersecurity-support.

Simons, Lynn, Rachel Holz, Melonia Da Gama, Gill Thomas, and Sean Doyle. 2022. "Can Closing the Cybersecurity Skills Gap Change the World?" World Economic Forum, March 10. https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap.

Starks, Tim. 2022. "Biden's Cyber Strategy Expected to Boost Federal Role in Protecting Critical Systems from Hackers." CyberScoop, July 14. https://www.cyberscoop.com/national-cyber-strategy-biden-drafting.

Tasheva, Iva. 2021. "Cybersecurity Post-COVID-19: Lessons Learned and Policy Recommendations." European View 20, no. 2: 140–49. https://doi.org/10.1177/17816858211059250.

Thomas, Douglas. 2020. "Evidence Suggests That the U.S. Loses Hundreds of Billions to Cybercrime, Possibly as Much as 1% to 4% of GDP Annually." US National Institute of Standards and Technology, May. https://www.nist.gov/news-events/news/2020/05/evidence-suggests-us-loses-hundreds-billions-cybercrime-possibly-much-1-4.

White House. 2016. "Cybersecurity National Action Plan." News release, February 9. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

Zabierek, Lauren, Felipe Bueno, Andrew Sady-Kennedy, Ngasuma Kanyeka, and Graham Kennis. 2021. "Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure." Belfer Center for Science and International Affairs, Harvard Kennedy School, August. https://www.belfercenter.org/publication/toward-collaborative-cyber-defense-and-enhanced-threat-intelligence-structure.

Endnotes

[1] Office of the President 2011; Schneider 2022.
[2] Minárik 2016; Schneider 2022.
[3] White House 2016.
[4] Schneider 2022.
[5] Rivero 2021.
[6] Schneider 2022.
[7] Edgar 2022b.
[8] Lonergan 2022.
[9] Lonergan 2022.
[10] Maschmeyer 2021.
[11] Lonergan 2022.
[12] Thomas 2020.
[13] Tasheva 2021.
[14] Maschmeyer 2022.
[15] Maschmeyer 2022, 17.
[16] Schneider 2022.
[17] Edgar 2022b.
[18] Starks 2022.
[19] Zabierek et al. 2021.
[20] Simons et al. 2022.
[21] Kennis and Zabierek 2022.
[22] Kennis and Zabierek 2022.
[23] Kennis and Zabierek 2022.
[24] Kennis and Zabierek 2022.
[25] Kennis and Zabierek 2022; Security Magazine 2022.
[26] Ratnam 2022; Reilly 2022.
[27] Schneider 2022, 11.
[28] Schneider 2022, 11.
[29] Edgar 2022b.
[30] Schneider 2022, 12.
[31] Edgar 2022a.
[32] McChrystal 2011.

#HISPBC

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

HOOVER INSTITUTION