Analysis of The National Cybersecurity Strategy March 2023

Shacara Pitre

Old Dominion University School of Cybersecurity

CYSE 525: Cyber Strategy and Policy

Professor Teresa Duvall

March 8, 2024

Analysis of The National Cybersecurity Strategy March 2023

Background

The Biden administration released the National Cybersecurity Strategy on March 2, 2023, which is a document that outlines the actions the administration will take in defending the digital world. This strategy replaces the 2018 Trump administration Cybersecurity Strategy. The updated version builds on the previous by continuing the focus on many of its priorities. In addition, the main difference between the National Cybersecurity Strategy and previous administrations is the unprecedented role that it designates for the federal government to play in the software market (Shankar, 2024). However, it seeks to carry forward and evolve many of the strategic efforts that were originally initiated by the 2008 Comprehensive National Cybersecurity Initiative (Jindal & Soliman, 2023).

Some of the key priorities of the strategy include: promoting multi-stakeholder cooperation with the private sector, international partners, and civil society organizations along with modernizing legacy systems, investing in critical and emerging technologies, etc. The strategy is aimed at shifting cyber defense responsibilities, disrupting cyber threat operations, and improving cyber resilience. It acknowledges that efforts by the private sector alone are insufficient when it comes to major cyber threats that are faced within the United States (Riggi, 2023). The National Cybersecurity Strategy drives the policy and action that the administration will take to defend the digital world. In addition, the strategy "...requires us to strike a careful balance between defending ourselves against urgent threats today and simultaneously planning strategically for, and investing in, a resilient digital future" (Coker Jr., 2024).

President Biden discussed how essential cybersecurity is to the functioning of the economy and how essential it is for critical infrastructure among other things. For instance,

Biden states “cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense” (Coker Jr., 2024). As a result, Biden explains how essential this strategy is in recognizing collaboration between public and private sectors in securing the world of cyberspace.

General Review

These principles shift the responsibility of protecting individuals, small businesses, state and local governments, and organizations, to the federal government and tech companies. Also, the National Cybersecurity Strategy promotes and encourages long term investments within cybersecurity and resilience. The National Cybersecurity Strategy is divided into five pillars:

- Defend Critical Infrastructure
- Disrupt and Dismantle Threat Actors
- Shape Market Forces to Drive Security and Resilience
- Invest in a Resilient Future
- Forge International Partnerships to Pursue Shared Goals

The pillars highlight a couple fundamental shifts which includes rebalancing the responsibility to defend cyberspace and realigning incentives to favor long-term investments. For clarity, “the digital ecosystem’s biggest, most capable, and best-positioned actors - be they in the public or private sectors - can and should assume a greater share of the burden for mitigating cyber risk” (U.S. Department of State, 2023). When entities across the public and private sectors face trade-offs, it is crucial that they have the resources, incentives, and capabilities to provide long-term solutions. The strategy gives a different take on the balance between the government

and private sectors when it comes to the roles and responsibilities needed to mitigate cyber risks. In addition, it recognizes the present realities that end users face with regards to reducing risks and seeks a legislative mechanism to enforce liability on providers when they fail to meet the basic security standards (Jindal & Soliman, 2023).

The National Cybersecurity Strategy places emphasis on the need for private entities to protect their systems from cyber-attacks. Along with this, the Biden administration highlights the need for investments from public sectors to assure the United States is able to continually stay ahead of the curve in modern technology and innovation while maintaining its global leadership role (Jindal & Soliman, 2023). The strategy emphasizes the U.S. working with its allies and partners to create a digital ecosystem that is defensible, value-aligned, and resilient. The goal of the National Cybersecurity Strategy is to protect the nation and digital systems from attacks that cause harm to the disruption of everyday American lives. It recognizes that cyberspace is a tool used to pursue higher aspirations and not as its own end (U.S. Department of State).

Pillar One: Defend Critical Infrastructure

The first pillar in the National Cybersecurity Strategy calls to defend critical infrastructure. This is crucial to our national security, economic prosperity, and public safety. Protecting critical infrastructure involves collaboration between the owners and operators along with having cybersecurity protections in place to address advanced threats (The White House, 2023). As a result, it would make it more difficult for adversaries to disrupt the infrastructures. Public and private sectors have made significant commitments to collaborative defense efforts. For instance, “the ‘shields up’ campaign preceding Russia’s 2022 brutal and unprovoked war on

Ukraine, to proactively increase preparedness and promote effective measures to combat malicious activity" (The White House, 2023).

It is important for federal agencies, product vendors and service providers, and stakeholders along with owners and operators of critical infrastructure, to collaborate effectively at speed and scale (The White House, 2023). Therefore, when incidents do occur, these groups are better equipped to handle the situation at large. Furthermore, the Federal Government is better equipped to support the defense of critical infrastructure when they are able to make their own systems more resilient and defensible. As a result, through the National Cybersecurity Strategy, the Federal Government hopes to be a model for critical infrastructure across the United States for how to successfully build and operate secure and resilient systems (The White House, 2023). The American people have a right to be aware of critical services affecting their lives and the nation's economy.

The marketplace today does not reward the owners and operators of critical infrastructure who invest in proactive measures to prevent and mitigate the effects of cyber-related incidents. This often puts them at a disadvantage. The strategy "...requires modern and nimble regulatory frameworks for cybersecurity tailored for each sector's risk profile, harmonized to reduce duplication, complementary to public-private collaboration, and cognizant of the cost of implementation" (The White House, 2023). Furthermore, improvement in new and updated cybersecurity regulations is necessary to meet the needs of national security and public safety. The Biden administration has made progress when it comes to this aspect by establishing cybersecurity requirements in key sectors, such as oil and natural gas pipelines.

In order for regulatory frameworks to be effective and efficient, they need to be put in place before a crisis, rather than waiting until after the crisis occurs through emergency

regulations (The White House, 2023). Critical sectors rely upon the cybersecurity and resilience of third party service providers. Therefore, cloud based services provide better, more economical cybersecurity practices at scale, but they are more essential to operational resilience across many critical infrastructure sectors (The White House, 2023). As a result, one of the goals of the Biden Administration is to identify gaps in authorities to drive better cybersecurity practices in the cloud computing industry along with other third party services. In addition, they work with industry, Congress, and regulators to close them (The White House, 2023).

The National Cybersecurity Strategy on a Global Scale

The White House seeks to strengthen ties with its partners around the world and support international institutions to confront the U.S. foreign adversaries, enforce norms of responsible state behavior in cyberspace, and safeguard global digital commerce and supply chains. Also, the Biden Administration lists nonprofits, civil society organizations, and local and regional entities as key partners in the fight against malicious cyber activity (Shankar, 2024). The strategy provides a framework for the U.S. to collaborate with its Middle Eastern partners to share threat intelligence and other critical information. Furthermore, the goal is to identify and address potential cyber-attacks before they occur. In addition, the U.S. can help build up its Middle Eastern partners' cyber capabilities through training and technical assistance (Jindal & Soliman, 2023). This involves establishing cyber defense teams, sharing cybersecurity best practices, and improving network security.

If they wanted to be advanced on cyber operations, the U.S. and regional partners could collaborate and conduct cyber exercises. This is to enhance their capabilities and coordination in responding to cyber-attacks from malicious actors. Also, they could develop norms of behavior

for cyberspace, promote regional cooperation on cybersecurity, and address the malicious use of cyber tools (Jindal & Soliman, 2023). Furthermore, ransomware attacks and other cybersecurity threats have negatively impacted the healthcare field.

The National Cybersecurity Strategy on Healthcare

Ransomware attacks along with other cyber-attacks have underlined the critical need for hospitals and health systems in their defense against malicious actors. The reason behind this is that healthcare contains a unique combination of highly targeted data sets that makes the field a prime target for cyber adversaries (Riggi, 2023). Hospitals and other healthcare facilities have to look at cybersecurity as an enterprise risk and not only as an IT related issue. Therefore, the National Cybersecurity Strategy recognizes several ideas that impact the healthcare system. They include: declaring ransomware attacks, conducting more offensive operations against cyber threat actors, and implementing software security requirements for software developers (Riggi, 2023).

Conclusion

In summary, the National Cybersecurity Strategy March 2023 lays the foundation for ways in which the U.S. and its allies can work together to create a safe environment for the digital world. With the rise in cyber threats daily, it is important for organizations, big or small, to have proper measures put in place to protect them from external threats. The Biden Administration explained how they can successfully tackle the growing threats digitally within the strategy. Overall, it is important that these issues are addressed at the federal level, so that state and local governments are better prepared to handle these situations.

References

Coker, H. (2024). *One Year In: The President's National Cybersecurity Strategy is Driving Change and Protecting the Nation.* The White House. https://www.whitehouse.gov/oncd/briefing-room/2024/03/04/national-cybersecurity-strategy-one-year/

Jindal, D. & Soliman, M. (2023). *The 2023 National Cybersecurity Strategy: How Does America Think About Cyberspace?* Middle East Institute. https://www.mei.edu/sites/default/files/2023-05/The%202023%20National%20Cybersecurity%20Strategy-%20How%20Does%20America%20Think%20About%20Cyberspace%3F.pdf

Riggi, J. (2023). *Why the Biden-Harris Administration's New National Cybersecurity Strategy Is an Important Step Forward for Health Care.* American Hospital Association. https://www.aha.org/cybersecurity/blog/why-biden-harris-administrations-new-national-cybersecurity-strategy-important-step-forward

Shankar, N. (2024). *The Biden Administration's National Cybersecurity Strategy: Opportunities & Challenges.* Middle East Institute. https://www.mei.edu/sites/default/files/2024-02/The%20Biden%20Administration%E2%80%99s%20National%20Cybersecurity%20Strategy%20-%20Opportunities%20and%20Challenges_0.pdf

The White House. (2023). *National Cybersecurity Strategy.* https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

U.S. Department of State. (2023). *Announcing the Release of the Administration's National Cybersecurity Strategy.* https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/