Diana Y Solorzano

CYSE 425W – Cyber Strategy and Policy

Professor Demirel, Hamza

Midterm Assignment

February 25, 2024

President Joe Biden explains in detail the reasoning and needs for the National Cybersecurity Strategy and how the five pillars listed in this document will not only strengthen our cybersecurity posture but also how the federal government will be stepping in and taking more responsibility as well. This document explains in detail how his administration will address and approach the goal of securing the United States' cyberspace. An important key to this strategy is that President Biden states that he has appointed government officials to bridge the gap with the private sector and will allow for the government to not only take more responsibilities in securing our cyberspace but also in setting a standard for cybersecurity structures and models.

The National Cybersecurity Strategy emphasizes the need for there to be more collaboration between private and public sectors especially when it comes to sharing information in order to be able to keep up with the amount of cyberattacks surfacing every day. It also explains that a majority of the responsibility for maintaining a secure cyberspace has been the responsibility of individual users and organizations rather than the government. The reasoning behind having the government more involved and be held more responsible for maintaining a secure cyberspace is justified as "we must ensure the Internet remains open, free, global, interoperable, reliable, and secure—anchored in universal values that respect human rights and fundamental freedoms" (National Cybersecurity Strategy, 2023, 03). Being that this is considered a human right and part of foundation freedom, it grants the government to take responsibility and actions in securing our cyberspace.

The National Cybersecurity Strategy explains that in order to keep up with the constant changes and advances in technology and cyber-attacks, the implementation of the five pillars is needed to best address these challenges on a government level. The five pillars listed in this

document are: (1) Defend Critical Infrastructure, (2) Disrupt and Dismantle Threat Actors, (3) Shape Market Forces to Drive Security and Resilience, (4) Invest in a Resilient Future, and (5) Forge International Partnerships to Pursue Shared Goals. Each one of these pillars works on establishing some type of communication with other communities to better defend and protect against cyberattacks.

The first pillar, 1. Defend Critical Infrastructure, focuses on protecting and securing our critical infrastructure. If these critical infrastructures were to be attacked or compromised, they could have detrimental effects on our nation. The need for collaboration between different sectors in order to reach standard regulations is explained in this pillar. The second pillar, 2. Disrupt and Dismantle Threat Actors, focuses on using the government's resources and capabilities to prevent malicious activity and sharing intelligence with other sectors in order to better report malicious activities. The third pillar, 3. Shape Market Forces to Drive Security and Resilience, focuses on putting more accountability on the markets that foster malicious activities. The fourth pillar, 4. Invest in a Resilient Future, focuses on the need to invest in a secure digital ecosystem and also addresses the issue of building on an existing faulty foundation. The fifth pillar, 5. Forge International Partnerships to Pursue Shared Goals, focuses on how we can improve the manner in which we approach and handle global cyber threats. This pillar also puts an emphasis on the need to have strong partnerships with international organizations in order to achieve the common goal of obtaining a secure cyberspace.

I will be explaining Pillar Two – Disrupt and Dismantle Threat Actors, more in-depth and the role it will play in the National Cybersecurity Strategy presented by President Joe Bidden. This pillar mainly focuses on what can be done on a national level by using diplomatic, information, military, financial, intelligence, and law enforcement efforts to "make malicious

actors incapable of mounting sustained cyber-enables campaigns that would threaten the national security or public safety of the United States" (National Cybersecurity Strategy, 2023, 18). An emphasis is put on the Federal Government to use its resources and capabilities to arrest, prosecute, and punish cybercriminals as well as the services cybercriminals use in order to prevent any further malicious activity. Pillar Two will be executed through five objectives: (1) Strategic Objective 2.1: Integrate Federal Disruption Activities, (2) Strategic Objective 2.2: Enhance Public-Private Operational Collaboration to Disrupt Adversaries, (3) Strategic Objective 2.3: Increase the Speed and Scale of Intelligence Sharing and Victim Notification, (4) Strategic Objective 2.4: Prevent Abuse of U.S. Based Infrastructure, and (5) Strategic Objective 2.5: Counter Cybercrime, Defeat Ransomware.

Strategic Objective 2.1: Integrate Federal Disruption Activities focuses on targeting online criminal infrastructure, services, and resources to the point where a malicious actor would be wasting their time trying to use them and make almost no profit, making these resources useless. This includes taking down known fraud campaigns, taking down botnets, taking down cryptocurrency used for ransomware, and then informing victims and organizations after the investigations have occurred to better protect.

Strategic Objective 2.2: Enhance Public-Private Operational Collaboration to Disrupt Adversaries focuses on federal agencies and private sectors working together in order to have a clearer understanding and representation of malicious activity occurring. By collaborating and working together, more information is spread amongst all sectors to better prepare and prevent these types of activities in the future. This objective encourages the private sector to work with nonprofit organizations since the amount of malicious cyber activity is too large for one type of organization to track.

Strategic Objective 2.3: Increase the Speed and Scale of Intelligence Sharing and Victim Notification focuses on not only sharing information between federal and non-federal partners but also focusing on doing it in a timely manner in order to stop cyber criminals and their activities. This objective explains how organizations that focus on this type of sharing, like the NSA Cybersecurity Collaboration Center's intelligence engagement, have dramatically helped stop malicious activity. It also states that cross-information sharing will allow victims to be notified much quicker and minimize the impact that identified intrusions can have.

Strategic Objective 2.4: Prevent Abuse of U.S. Based Infrastructure focuses on how the Federal Government will need to work with different infrastructures in order to quickly identify malicious activity using these infrastructures. Besides collaborating with different infrastructures, victims will also be encouraged to make reporting through the creation of an easier system. This will aid in the prevention of malicious users using these resources in the future. This objective will also hold service providers accountable for how their services are being used in order to prevent abuse.

Strategic Objective 2.5: Counter Cybercrime, Defeat Ransomware focuses on the negative impact that ransomware has on every aspect of our nation and the difficulty in stopping these attacks and prosecuting the cybercriminals behind them. This objective describes how the U.S. will implement the following four efforts: "(1) leveraging international cooperation to disrupt the ransomware ecosystem and isolate those countries that provide safe havens for criminals; (2) investigating ransomware crimes and using law enforcement and other authorities to disrupt ransomware infrastructure and actors; (3) bolstering critical infrastructure resilience to withstand ransomware attacks; and (4) addressing the abuse of virtual currency to launder ransom payments" (National Cybersecurity Strategy, 2023, 21) as a counter to ransomware.

Resources

National Cybersecurity Strategy. National Cybersecurity Strategy 2023. (2023, March 1). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf