Midterm Assignment

The National Cybersecurity Strategy May 2024 (Version 2)

Jade Ames Moore

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy & Policy

Dr. Hamza Demirel

March 2, 2025

Abstract

With the development of cybersecurity and the digital world, there will always be a flaw. Cyber threats have grown independently, locally, as a nation, and worldwide. With this pressing issue we need to implement and protect cybersecurity as a team, not separated. It took terrorist attacks and the lack of protection on critical components to get where we are now with The National Cybersecurity Strategy May 2024. Over the year The National Cybersecurity strategy has been revised based on who was the commander in chief of armed forces at the time. When President Trump was the president in 2018, his initiative was to focus more on offense and defense cyber capabilities. The Biden-Harris administration focused more on defending cyberspace from us individuals and smaller entities. Based on the following document of **The National Cybersecurity Strategy May 2024 (Version 2):**

> Achieving the vision set forth in the Strategy involves two fundamental shifts in cyberspace: rebalancing the responsibility to defend cyberspace onto more capable actors; and realigning incentives to favor long-term investments in cybersecurity and resilience. (p.4)

This updated version also goes over the 100+ initiatives that were aimed at enhancing the nation's cybersecurity position. When cyberthreats were first coming to light, defending and protecting critical infrastructure started with the head of Government, military plans, energy, and water systems. Based on The National Cybersecurity Strategy May 2024 (Version 2) Critical Infostructure now depends more on Hospitals, Public Health, safety, and the National Economy. It enhances the collaboration of all sectors (private, public, Institutions) to work and

communicate among each other. If we can't all be on the same page and goals on protecting our nation, it will become more difficult to create resilience. That being said, we all need to work together, individuals included. Starting at the root of a problem can help in the long run, that's why we need awareness and education, and this strategy goes over that also. When it comes to goals and wanting to succeed in this future achievement, it comes with deadlines, budgeting, and responsibility, especially when everyone can be affected.

In this NCS updated version we can access the government's goal and plans. For example, they are looking into upgrading the National Cyber In incident response plan. Based on the document of the National Cybersecurity Strategy on page 22, with the collaboration ONCD, they plan on strengthening the process, procedures, and systems for all external partnerships to use their roles and capabilities. Another goal that comes with this document is redirecting Juvenile cybercriminals. With unlimited access to the internet, if they break that door, they can expose children or young adults to curiosity. Juvenile cybercriminals can also find themselves in the predicament due to the cause of peer pressure from peers, easy money, or the lack of knowledge on consequences. In some cybercriminal's logic, if they're not doing anything physical to hurt someone, then what they're doing digitally want cause that much damage, especially a Juvenile.

All these factors I've spoken on come from are bits of pieces the NCS supports through the five pillars. The first Pillar, Defend Critical Infostructures, second Disrupt and Dismantle Threats, third Shape Market Forces to Drive Security and Resilience, fourth Invest in Reliant future, and the Fifth and final Pillar Forge International Partnerships to Pursue Shared Goals. To choose one Pillar I favor and believe will succeed the nations' final goal would be Pillar Three: Shape Market Forces to Drive Security and Resilience.

During my time in this class I've noticed something that other countries have, and we don't, a data privacy law. Data privacy is a huge issue in the United States. We are behind when it comes to this topic, yet other countries and better yet, states have a law to protect induvial information. For example, Europe has the General Data Protection Regulation that sets high standards for Data protection and how individuals have their rights to their own data. There is also the law in California, The California Consumer Privacy Act stating the consumers have the right to access, correct, and delete their personal data. Making a law for privacy rights can earn citizens trust for ensuring responsible data handling, can reduce the risk of breaches, and innovation.

When I went over the NCS document and saw the third Pillar, Shape Market Forces to Drive Security and Resilience, I saw the opportunity of decreasing risks, gaining trust, and also holding these companies to an accountably when cyber breaches occur and everyone supporting that companies have now been exposed. One of the many initiatives that comes with this goal is Develop a U.S. Government IoT security labeling program. Working with the federal communications commission, they will make a secuity labeling program that will be called "U.S Cyber Trust Mark" to products that have been verified and up to standards when it comes to cyber ethics of a device/company. The benefits for this initiative would enhance national security, when we think of what we use in Hospitals or out that digital, such as implantable devices (pacemakers), Hospital Network and Systems, health records, communication systems would all need to meet a certain criterion and could save many live. This can also help with international collaborations, other countires seeing what we are trying to do to make a difference could help in the long run we all collab with ideas. This could also save years of research.

Nothing is free. So, when their brainstorming ideas to help cybersecurity as a nation, we also must figure out funding to do this research. In this case they would use Federal Grants and

Other Incentives to Build in Security. Based on the National Cybersecurity Strategy on page 41, initiative number 3.4.3, Prioritize cybersecurity research, development, and demonstration on social, behavioral, and economic research in cybersecurity. Through a grant reward in 2024, the National Science Foundation was made to prioritize increasing understanding of society and individuals' impact on cybersecurity threats and how we can overcome them. The research will look over ethics, cyber economics, human factors, and anything else that can cause cybersecurity downfall.

All Five Pillars have an important role when it comes to protecting cyberspace and finding ways to improve 10x harder than the cyber threat. At this moment right now, someone is actively doing a cyber malicious act, we just need to know how to find and stop them, make sure they know the consequences, and use them as an example to educate individuals. We are also setting ourselves up as an example when it comes to international collaboration when it comes down to research. Everyone all around can improve their cyber hygiene, but we all need a plan and something to look up to.

National Cybersecurity Strategy Implementation Plan. (2024, May). The National Cybersecurity Strategy May 2024 (Version 2)