National Cybersecurity Strategy of the United States

Brandon Zachary Pearson

Old Dominion University

CYSE425W - CYBER STRATEGY AND POLICY

Professor Malik A. Gladden

September 17, 2023

Within the last 20 years, the Internet has changed drastically. The development of the Internet has changed the way we engage with each other and allowed for new opportunities. With the rapid expansion of the Internet, it has introduced many problems as well as concerns. Anything that comes about in a quick manner often has issues later on that have to be solved or addressed. In the Interenets case security wasn't accounted for in the beginning. This later became an issue with the prevalence of cyberattacks and hackers. These attackers take advantage of the lack of development of security and policies around cyber security. Over the past 15 years, there has been a strong push to develop cyber strategies and policies in the United States. The National Cybersecurity Strategy of the United States "NCSS" was created in order to address the issue of cybersecurity in the U.S.

The National Cybersecurity Strategy was published in 2023, with the goal of creating a safer cyberspace. The goal was to accomplish this without hindering or impeding freedom and internet accessibility. The Internet falls under a critical infrastructure meaning it is vital to have in order for things to function. The increasing number of IoT devices connecting to cyberspace has changed the importance of the nation's critical infrastructure. The infrastructures that will be impacted are electrical grid systems, transportation, and telecommunications. (Johnson p.43) Leading to why this is an important thing to implement. The NCSS can be broken down into five pillars that each have sub-strategies within them. The main five pillars in order are: defend critical infrastructure, disrupt and dismantle threat actors, shape market force to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals.

The NCCS was developed due to the desire to protect the United States from bad actors or foreign nations. In recent years cyberattacks have become more relevant which has sparked

the need for a stronger plan. Notable cyberattacks in recent times were the Colonial Pipeline ransomware attack and Killnet. These two cyberattacks showcase the impact a cyberattack can have on critical infrastructure. Additionally, Russia's attack on Ukraine in 2022 aided in the development of the NCSS. The threat of cyber-attacks has grown over the years it is heavily believed that most wars will be done using cyber warfare in the future. This is due to the ability to cause a wide range of harm for a lot less effort and money. The NCSS sets forth policies that should help in ensuring a safer cyberspace. These policies can help government agencies protect critical systems and internal operations. In the Colonial Pipeline situation, the NCSS set forth better procedures that could have limited the impact of the cyberattack. Potentially, if the policies were created before it would have not occurred. "A more promising approach to cybersecurity for critical infrastructure involves deep collaboration between industry and government to better align efforts." (Atkins, p.774). The difficult part of implementing the strategy is due to the collaboration it will take between many different industries. The government also wants to implement these strategies without impeding which can cause things to not get done efficiently.

The NCSS was created to address cyberspace and the issues that have arisen with the Internet. The strategy was created to support other national policies such as economics, foreign, and public awareness. NCSS fits into these policies by addressing the impact and issues that come about due to the internet. Economics is heavily reliant on the Internet and digital currency. Economics policies and cyber polices work together to prevent theft and fraud due to cyber incidents. Foreign policy and cyber policies align in trying to make sure foreign business and interaction take place ethically. Keeping nations accountable and ensuring that no side is doing unethical things. Additionally, the U.S. works together with foreign nations to counter common threats and maintain a transnational Internet (NCSS, p.27).

The National Cybersecurity Strategy of the United States is a great addition to the policies that surround the Internet. It hopefully will create a safer cyberspace for citizens as well as companies. Through the implementation of the strategies that are given in the NCSS agencies should be able to protect themselves from cyberattacks. In order for NCSS to be effective it will take cooperation amongst the government and citizens.

Refernces

Atkins, S., & Lawson, C. (2022). Integration of Effort: Securing Critical Infrastructure from Cyberattack. Public Administration Review, 82(4), 771–775.

Johnson, T. (2015). Cybersecurity : Protecting critical infrastructures from cyber attack and cyber warfare / (First ed.). Boca Raton, FL :: CRC Press, an imprint of Taylor and Francis.

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