Analysis Of National Cyber Security Strategy March 2023

Midterm Assignment

Chris Evans

01206431

School of Cybersecurity, Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Prof. Hamza Demirel

March 15, 2023

The United States National Cyber Security Strategy 2023 (NCSS) is a plan developed by the Biden White House including input from multiple stakeholders in the private sector along with government departments, on how to improve and strengthen the cyber security of US based private and government computer networks, as well how to better coordinate government resources and industry leaders to deter and prosecute cybercriminals , hackers, and rogue nation states who launch attacks against American interests (NCSS, 2023). This is the most current revision of this document which has existed since its initial inception as the National Strategy to Secure Cyberspace publish in 2003 as a response to the 9/11 terrorist attacks on the United States (Secure Cyberspace). The NCSS attempts to tackle the large problem that many of the responsibilities of cybersecurity are given to small departments or individuals in small organizations while the threats they face are often numerous in quantity and often resource rich. The goal of the NCSS is to help ease this burden on smaller organizations and shift the responsibility to larger more resources rich and knowledgeable defenders as well as all levels of government. Government hopes to create collaboration with stakeholders to create a better cybersecurity ecosystem where incentives are driving long term security investments, resilience, and new technology as well as training future users and IT personnel (NCSS).

A major goal of the NCSS is to build off existing cybersecurity, technological, and regulatory achievements of the private and public sector. The NCSS will leverage experienced private sector leadership and existing governmental policies and laws to create informed and technologically sophisticated responses to attacks as well as to forge a path to achieve the NCSS strategic goals. Creating a favorable strategic environment is another goal of the NCSS and will include responding to and shaping trends in how technologies are used and how interdependent systems are secured. Reliance on these interconnected computer systems and infrastructure

increases daily and has a human, economic, strategic cost when they are disrupted, destroyed, or compromised by malicious actors. Ensuring that the digital world is secure is necessary for continued national security and prosperity of the United States. The strategic environment also includes dealing with malicious actors who may be seeking monetary gain as in cybercriminals, or to achieve political ends as the advanced persistent threats of countries like China, Russia, Iran, and North Korea. Hostile countries like those have sought to disrupt US based infrastructure and economics as well as to commit cyber espionage or influence campaigns. Cybercriminals using ransomware have created billions of dollars of economic losses, and disrupted operations of infrastructure, schools, and healthcare organizations (Widakuswara). Building resilience in cyberspace is another goal of NCSS, and will include collaboration again between all US stakeholders who require secure cyberspace to operate in. Government hopes to take more of the responsibility to defend cyberspace off of small organizations and instead ask the best positioned actors to create more secure resilient cyberspace. Actors like technology providers and builders are brought to the table to create safer systems and methods to secure networks, while governmental entities provide threat intelligence gathering, and disrupt cyber threats as they can. Together the goal is to try to create safer and more resilient systems with all stake holders contributing to the strategic vision. A major part of the NCSS deals with creating and improving collaboration around five pillars. The first pillar is to Defend Critical Infrastructure. The second pillar is to Disrupt and Dismantle Threat Actors. The third pillar is to Shape market Forces to Drive Security and Resilience. The fourth pilar is to Invest in a Resilient Future. The fifth and final pillar is to Forge International Partnerships. Below we will briefly outline the pillars goals, and strategic considerations (NCSS).

Defending critical infrastructure is the first pillar and will include creating harmonized regulations that can be used as well as allowing stakeholders to collaborate to share support with each other. Government agencies will offer their updated and improved capabilities to help improve cybersecurity of critical infrastructure as well.

Disrupting and dismantling threat actors is the second pillar and will be achieve through integrating federal disruption activities that share information on threat actors and increase speed at which the intelligence can be shared with the affected parties or sectors. This will also coincide with increased law enforcement activity and Department of Defense activity to find and eliminate threat actors. Special considerations will be focused on eliminating ransomware activities.

Shape market forces to drive security and resilience is the third pillar which aims to promote practices which enhance security in the market by adopting best practices and shifting responsibility to those best able to defend computer systems. The usage of Federal purchasing power and grants will be the main source of incentives (NCSS).

Invest in a resilient future is the fourth pillar and seeks to invest in technical and digital future by refunding research into digital infrastructure and technologies as well as education to create the future cybersecurity and technology literate citizens who will create and maintain future computer infrastructure. This will begin with fixing security issues currently known and then preparing for future challenges.

Forge international partnerships is the fifth and final pillar and includes working with other countries to expand and enforce cybersecurity regulations and standards as well as shape international accountability for malicious behavior. This will include working with countries to

increase their cybersecurity and to secure global supply chains to prevent attacks at the procurement level.

Pillar two, Disrupt and Dismantle Threat Actors seeks to combine all the diplomatic, information, military, financial, intelligence, and law enforcement capabilities of the US to deter and eliminate malicious actors' attacks on the United States government and US based computer systems and organizations (NCSS). The Federal government and non-government entities have worked and will continue to work together to respond to cyber incidents. Cyber criminals have been prosecuted and state sponsored attackers have led to sanctions on rogue states in attempts to limit resources available for cyber-attacks.

NCSS envisions law enforcement disruption activities of cyber crime being constant and focused on attempts to deter attackers. These disruption activities by DoD, DOJ, and the Intelligence communities have benefited already by removing criminal infrastructures and activities and by sharing relevant information like malware signatures with vulnerable stakeholders, enhancing diplomatic efforts with other nations, and assisting intelligence operations (NCSS).

Further assisting the disruption activities is public-private collaboration. Because of the large amounts of private sector cybersecurity work, the ability to share information from one private sector to another or one private sector company to all other companies in the sector is incalculably valuable. This cooperation has had previous successes and it is a goal to continue leveraging this talent to continue disruption operations. The private sector is encouraged to continue sharing their knowledge and multiplying their efforts with collaborative activities.

All the information in the world is not helpful unless the speed and scale of threat intelligence and victim notification is not increased. The NCSS is committed to enhancing the speed of collaborative efforts and continuing successful efforts like the NSA Cybersecurity Collaboration Center. Additionally, CISA working with the FBI has made great advances in quickly notifying victims. The Federal government aims to continue and increase this progress by expanding the threat information to more stakeholders.

The exploitation of US based infrastructure also is a major avenue for threat actors and one NCSS seeks to limit. Cloud infrastructure and other digital services have been used to commit criminal acts or attacks against US firms, or governments. The federal government will work with these technology providers to help them identify when these resources are used by attackers as well as share the information so that other potential organizations can be vigilant against this behavior (NCSS).

Disrupting ransomware is a chief concern as it threatens all levels of society. Schools, hospitals, energy production, and government resources have all been disrupted by ransomware attacks. The FBI and CISA have created the Joint Ransomware Task Force (JRTF) to coordinate disruption campaigns against ransomware actors. The US will continue to use all its influence and international cooperation with its partners to disrupt and prosecute ransomware attacks as well as remove resources and loopholes attackers use. This includes limiting and regulating financial services as well as cryptocurrency exchanges. Payment of the ransoms is strongly discouraged, and reports of ransomware attacks should be shared with law enforcement to prevent further attacks.

While this strategy is very similar to the one that it replaces there is a shift in major ideology. Once change is that now the federal government seems focused on creating a bigger regulatory framework and taking more of the responsibility of cyber security off of the private sector and putting it on larger organization and the government itself. This is a big challenge as many organizations will have to learn to navigate the regulatory framework and begin upgrading their cybersecurity postures. Another shift is that the federal government seems more willing to take a stronger active role in disrupting threat actors by use of all its tools of power (Lin). And most striking is that the federal government will view ransomware as national security threat rather than as a crime. This has profound implications for diplomacy and for law enforcement interactions across the board (Widakuswara).

CITATIONS

Lin, Herb. (2023). *Where the New National CyberSecurity Strategy Differs From Past Practice.* LawfareBlog. Accessed Mar, 2023. https://www.lawfareblog.com/where-new-national-cybersecurity-strategy-differs-past-practice

National Cyber Security Strategy March 2023. (2023). *White House*. Accessed Mar, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

National Strategy to Secure Cyberspace February 2003. (2003). *CISA.* Accessed Mar, 2023. https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

Widakuswara, Patsy. (2023). *US Launches Aggressive National Cybersecurity Strategy.* VOANews. Accessed Mar, 2023. https://www.voanews.com/a/us-launches-aggressive-national-cybersecurity-strategy-/6986279.html