CYSE 425 Midterm Assignment

Latitus Jones

October 31st, 2024

The National Cybersecurity Strategy is an important step in the direction of creating an entirely safe and secure cyberspace for the American people. Its goal is to create “a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences (White House, 2023).” Cyber threats have dramatically increased since the onset of the COVID-19 pandemic due to the increased volume of technology use with people in their homes. This has led to a tremendous challenge for cybersecurity due to the need of the field outpacing the demand for trained professionals. Therefore, this strategy was created to remove the constant fear away from individuals and onto trained and reputable organizations. Within the strategy, the White House outlines five pillars each with its own set of goals and implications for cyberspace.

The first pillar is to defend critical infrastructure which involves power grids, water supplies, transportation services, and health services. If compromised, this could lead to incredible amounts of panic for the American people as the core services of daily life become unsafe and unreliable. It would also less to distrust as the company’s reputation would be tarnished due to the unsafe security habits that led to the incident. With help from the government, this issue could be much more secure due to the unlimited resources available and professional talent involved.

The second pillar is to disrupt and dismantle threat actors which consists of taking the power away from the dangerous attackers. This threat could range from multiple sources whether it be a single person in a basement or a whole team of seasoned professionals in another country. However, this pillar is made to take the power back from them by making advancements in

identifying and disrupting their actions to protect the American people. Strategies to do so could include intel sharing or law enforcement cooperation.

The third pillar is to shape market forces to drive security and resilience which is the government equipping American organizations with the tools to have better rules and policies for internet security. With this approach, it also allows for the businesses to receive incentives for their compliance and it could lead to further improvements to their systems. Frameworks like the NIST framework are widely known in cyberspace and they can lead to significant advantages if followed for any business. There is also a non-financial incentive as companies could raise consumer awareness of the compliance which could enhance consumer trust.

The fourth pillar is to invest in a resilient future which is an approach that could include several different avenues for strengthening security. Currently, there are countless ways to manipulate a system especially with the emergence of artificial intelligence. This could lead to extensive ramifications for companies due to the extreme intelligence of the technology, however, with the right investments it could also help as well. By investing in AI and other forms of automation, it could lead to incredible advancements in cybersecurity around the world.

The final pillar is to forge international partnerships to pursue shared goals which is an incredibly successful strategy since attacks happen from all over the world. This strategy has been notable with the creation of the General Data Protection Regulation and the partial compliance of the United States. While it is not our policy, it has aided immensely with how it affects global businesses that also operate in the United States. Collaboration efforts like this could make it much easier to end this cybersecurity crisis around the planet.

The NCS has a profound effect on the world and it could lead to major progress in this increasingly digital world. However, all must do their part in order to remain aware and safe.

The pillar that this essay will focus on is to forge international partnerships to pursue shared goals. When thinking about this pillar, it has implications that could aid cyberspace in its entirety rather than just for a particular country. Collaboration amongst countries could lead to frameworks like NIST and policies like the GDPR becoming common practices for companies leading to a more safe environment for all around the world. Countries could also aid in security investments which could offput the extreme financial burden that implementing cybersecurity measures could pose. A few objectives defined within the pillar include building coalitions to counter threats to our digital ecosystem, strengthening international partner capacity, and expanding United States ability to assist allies and partners (White House, 2023).

Objective one is a critical point that must be evaluated in order to create a functional defense that is able to be implemented around the world. Building coalitions may be temporary in nature, however, it could lead to permanent effects that help all parties involved. An example of this would be the Declaration for the Future of the Internet which was launched in April 2022 by the United States and sixty other countries (White House, 2023). Since the creation of the DFI, there have been several other coalitions created like the Freedom Online Coalition and it has promoted "secure and trusted data flows, respects privacy, promotes human rights, and enables progress on broader challenges (White House, 2023)." Coalitions have proven to be a great way to forge a common goal into reality amongst unlikely partners which has really benefited cyberspace.

The second objective is vital due to how it allows for collaboration to lead to execution and progress for the countries involved. It gives the ability for the US to "enable our allies and partners to secure critical infrastructure networks, build effective incident detection and response capabilities, share cyber threat information, …and support our shared interests in cyberspace

(White House 2023).” These collective efforts not only enhance the trust of allies, but it also allows for a stronger system to be made due to the minds of both countries coming together to implement a similar goal. Developing these connections can further the progress of this goal as well since it could allow for mutual and unlikely allies with common goals to be willing to join and increase the partner volume. Partner capacity is a key future in assuring the pillar is able to create positive universal ramifications for the beneficiaries.

The final objective is important as it has to deal with how the allies communicate and more specifically how the US can reach and expand the policies created. The White House describes how countries like Puerto Rico, Albania, and Montenegro look to the United States for support in order to conduct investigations, responses, and then recovery plans after a cyberattack. This dependence on the US not only helps us give to a less fortunate country, but it also allows for us to implement our high cybersecurity standards into their system to protect against future attacks. There are also other efforts being made to expand the overall reach as the US is looking to “build a virtual cyber incident support capability that enables Allies to more effectively and efficiently support each other in response to significant malicious cyber activities (White House, 2023).” With this objective being followed, there could be significant improvements on the communication front for all that are involved which could further the forged bonds amongst the countries.

Pillar Five of the National Cybersecurity Strategy is crucial to the success of the entire process of creating a more secure cyberspace. It promotes a new initiative for collaboration unlike any other pillars which can give way to partnerships and ideas that create unprecedented change. Individual goals which would have taken years for a single country can be done more efficiently and effectively in a matter of months as this strategy continues to evolve.

References

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