Midterm Assignment

Hunter Bishop

3/19/23

Professor Hamza Demirel

Old Dominion University

CYSE 425W

The National Cybersecurity Strategy March 2023 seems to be a big step in the right direction, especially for citizens who do not have much knowledge of the cybersecurity field. The government is looking to centralize efforts in cyber defense so that individuals are not forced to try and work out how to best defend themselves and keep their information safe. The National Cybersecurity Strategy March 2023 has laid out five “pillars” of their plan by which they will do this which are: defend critical infrastructure, disrupt and dismantle threat actors, shape market forces to drive security and resilience, invest in a resilient future, and forge international partnerships to pursue shared goals. These five pillars are meant to be the guiding principle by which the United States as a country strives to better protect information and stop cyberattacks moving into the future. The National Cybersecurity Strategy acknowledges that not only the United States but “the world is entering a new phase of deepening digital dependencies” (National Cybersecurity Strategy, 2023). As technology continues to advance, so will the threats posed by attackers who wish to take advantage of that. The National Cybersecurity Strategy has dedicated an entire pillar of focus to that question in their “disrupt and dismantle threat actors” pillar. By stopping threat actors, it increases not only security at a national level, but also security at an individual level. If the National Cybersecurity Strategy is implemented as planned, then the organizations who offer the best defenses against cyberattacks of all kinds will be called upon to help people who are unable to defend themselves due to whatever reason be it cost or lack of knowledge. The United States has a pillar dedicated to forging international partnerships, but they will also be trying to forge partnerships with businesses in the country that are able to help their goals and to help defend their potential consumers as well. With the rapid advancement of technology, the rule of thumb seems to be that attackers are always a step ahead, but by pooling the resources and brain power of people from many countries and many backgrounds around the world, the hope is that the combined forces on defense will be able to outwit attackers and create robust and resilient defenses. One of the more common words in the National Cybersecurity Strategy March 2023 is the many forms of the word *resilient*. The Oxford dictionary defines resilience as “the capacity to withstand or recover quickly from difficulties.” In building a more resilient structure for cyber defense, the National Cybersecurity Strategy knows that organizations and other countries might not be willing to help without some incentive for themselves, and that has already seemingly been accounted for in this document by highlighting the necessity of a more secure world that will be beneficial to everybody in it. Cybersecurity is still a relatively new field and is growing rapidly which is why the National Cybersecurity Strategy wants to establish measures that will be able to last for a long time, or will be flexible enough to change with the advancement and creation of new technologies. The incentives they create for organizations who comply with and work with the government will also be focused towards creating long-term solutions. Overall, the National Cybersecurity Strategy March 2023 is a good starting point for the future of cyber defense and information security. The five pillars that have been laid out are all necessities if the National Cybersecurity Strategy wants to “rebalance the responsibility to defend cyberspace” (National Cybersecurity Strategy, 2023). Implementing these plans will not be a quick process by any means, but that is why it is paramount for the government of the United States and other countries to begin their work with each other and the private organizations within so that eventually, the burden of cyber defense will no longer be in the hands of individuals, but rather in the hands of those who are best equipped to defend cyberspace.

One of the most important things when creating new policies and trying to establish new systems is making sure that they will be effective in the future or that they are flexible enough to be molded towards the future. That is why pillar four of the National Cybersecurity Strategy March 2023, invest in a resilient future, should be one of the top focuses for the governments and businesses that are cooperating to make cyberspace a safer and more secure environment (National Cybersecurity Strategy, 2023). Investing in a resilient future will inevitably have some shortcomings as the plans that are made now are likely going to be obsoleted by the technological advancement of the years following. This is why the plans must also be flexible. The National Cybersecurity Strategy 2023 has already addressed this in their objective 4.3 and objective 4.4 which plan for the future after quantum computing is idealized and the future in which clean energy is more abundantly used, respectively (National Cybersecurity Strategy, 2023). Quantum computing is the obvious direction for cybersecurity to trend towards as many of the top experts in the field continue to work on ways to make it more available, so it will be necessary to take it into account when planning for a resilient future. With quantum computing comes quantum encryption which would be an excellent tool that can be used to greatly increase information security, therefore fortifying cyberspace. And as clean energy becomes more widely used, it will likely require more automation and more complex systems to take advantage of which will come with a cybersecurity risk. So in objective 4.4, the National Cybersecurity Strategy 2023 explains that as opposed to the more common method of securing something after the fact, the government will employ an organization they call the National Cyber-Informed Engineering Strategy to create a security infrastructure for clean energy sources and it will allow the government to be ahead of the game in terms of cyber defense of these critical systems (National Cybersecurity Strategy, 2023).   As previously mentioned, attackers always seem to be a few steps ahead of cyber defense professionals, so this is a step in the right direction to being at least on par with the defenders, and hopefully ruling out zero-day attacks for clean energy systems. Another important thing addressed by the National Cybersecurity Strategy 2023 is addressed in objective 4.6, develop a national strategy to strengthen our cyber workforce (National Cybersecurity Strategy, 2023). As the United States, and the world in general, continues to become more reliant on technology and the interconnectedness of it, there will be an increasing need for workers in the field of cybersecurity. Many attackers are opportunistic, and those type of attacks will hopefully be reduced to almost none as the world closes in on a more resilient cyberspace, but the more dangerous attackers are the ones that have the backing of an organization or a nation-state. The most intelligent and best minds will be needed to come up with ways to establish resilience and to keep it, and this objective 4.6 is addressing that issue. The National Cybersecurity Strategy 2023 aims to increase diversity in the cybersecurity field and to widen the talent pool that businesses and governments pull from (National Cybersecurity Strategy, 2023). Overall, this fourth pillar will end up being one of, if not the single, most important tasks that the National Cybersecurity Strategy 2023 aims to take on. Creating a more resilient future is a difficult task and will be made more difficult by the contradicting desires of all the parties involved. If a balance is struck and different countries and organizations are able to collaborate effectively, cyberspace will see rapid and major improvements to information security and quality of life. If the National Cybersecurity Strategy 2023 is to accomplish its aim with creating resilience, then it will require effort from all over the world, from people of many different backgrounds. This way, the voices of different minorities and majorities around the world can be heard and accounted for in making cyberspace a place that is secure and welcoming to anyone.

References

National Cybersecurity Strategy. 2023, www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.