National Cybersecurity Strategy Analysis

Dae'lyn Bellamy

Department of cybersecurity

CYSE 425W

Professor Hamza Damirel

Today I will be conducting an analysis of the May 2024 National cybersecurity strategy that was released by the biden administration and more specifically I will be going over one of the Pillars laid out in this strategy "disrupt and dismantle threat actors". I have decided to look into this Pillar more carefully because I believe that it is beneficial for people to know and understand how the government plans to tackle and limit the amount of cyber threats not only posed to the country but also your average civilian that may not know or understand the tools the government is planning to use to protect them and how they will be using those tools. Now This paper will consist of Five different sections not including the introduction. A summary of the strategy, the need for this strategy, analysis of our chosen Pillar "disrupt and dismantle threat actors", the impact of this pillar, and lastly the conclusion. Now let us begin with a quick summary of the national cybersecurity strategy.

In this strategy released by the biden administration has one overall goal and that is to create tools that will strengthen, secure and make the United states critical infrastructures more resilient to cyber attacks, something that is very much needed in today's world especially with recent cyber attacks such as the solar winds attack that was able to gain access to millions of civilian and government computer world wide. With this new strategy attacks like that will become much harder and less common overall. This updated and improved cybersecurity strategy is trying to imply an interestingly new plan to help better this country, which is to distribute cybersecurity roles and responsibilities to companies and agencies who are best suited to handle such responsibilities. This allows the United states to ensure that its cyber defense is always being managed by some of the best people within the field, this also means a

decrease in government bureaucracy involving implementation of new technologies into the cyber domain and of course to make this all work the strategy includes over 100 key initiatives for 18 different agency within the government such as the department of homeland security, the cybersecurity and infrastructure security agency, and the department of defense where are some of the agency involved in making this strategy successful with the hopes of strengthening public and private sector corporations, ensuring a strong cyberdefense for our critical and supply chain infrastructure, fighting cybercrime more effectively and more quickly, allowing for the development of more powerful cybersecurity technologies and even allowing for a larger cybersecurity workforce to enable all of this to be possible in the first place.

Of course for a plan this grand and encompassing there would have to be some kind of oversight to ensure that everything is going as planned and the agency responsible for that would be the office of national cyber director. Overall this strategy lays out the groundwork for a highly successful and potent security framework that will ensure our countries security within the cyber domain for years to come and even if only a few of the things mentioned within this strategy ever come to fruition it will still stand to be quite substantial for increasing our cybersecurity throughout the whole nation. Now that you have a basic understanding of what this new cyber defense policy is trying to accomplish, let us now explain why such a thing is required in the first place in more depth.

A cyber defense policy like this is needed to ensure events like the previously mentioned solarwinds attack are never able to happen again. An attack of that magnatured could have been far far worse than it was if the culprits had intended to

conduct a first strike against this country with the intent to cripple us. The threat and frequency of cyberattack will only grow as adversary nations become stronger and more advanced. This strategy isn't just needed to protect us against enemy nations though it is also very helpful in protecting us against highly competent and skilled cyber criminals who are taking advantage of the ever rapidly growing technological dependence our society has come to rely on with digital technologies. With all of this in mind it is obvious that our future is one of near constant cyberwarfare either against other nations or against individual or group actors and this strategy for a more secure cyber domain will become extremely important for everyone's future in this country. Now that you know why this plan is important we should now go over our specific pillar we are going to analyze today being the pillar of "disrupt and dismantle threat actors".

This is the second pillar of the biden's administration's new cybersecurity strategy and it aims to proactively huntdown and target,disrupt, and dismantle adversary threat actors before they are able to threaten the United states cyber domain. Pillar two seeks to develop a strong defense against cyber attacks but also develop the technologies to effectively fight back against the individuals, organizations, or nations that are behind such attacks. In order to accomplish this the Pillar outlines different tactics the united states will take to ensure cyber dominance whether it be in the defense or offensives such tactics include increasing intelligence sharing amongst different agencies, development of stronger offensive cyber tools, and the targeting of financial and operations support chains which will help disrupt their ability to fund and gather resources for their cyber operations. All of this is critical in this strategy succeeding what it was created to do because it mandates ways to further develop and strengthen our

ability to defend and against cyber attacks and deepen our ability to work together between many different organizations and agencies to ensure we are approaching a threat in the best possible way. Now that you know what this pillar of the cybersecurity strategy seeks to achieve let us now discuss the impact this pillar will have on our cyber defense and offensive abilities.

The impact this pillar will have on our ability to conduct cyber defense and offensive is substantial. This pillar will give the united states the ability to proactively hunt down and eliminate cyber threats even before they make themselves known which is extremely important in the world of cyber security because you don't want to know about an attack as its happening so being able to stop it before its able to be launched is very important. This Pillar will also have a large impact on federal agency and corporation cooperation as it will lead to more effective communication and teamwork amongst each other which will allow for an effective cyber defense to be put up for not only companies but the government as well.

In summary, this National cybersecurity strategy implementation plan puts forwards multiple different plans and systems in place to ensure that the united states will be able to protect itself and its citizens from cyber attacks, which is becoming increasingly important in our growing digital based world with more and more things coming to rely on digital technologies and also becoming more vulnerable to cyber attacks. With this strategy implemented it poses a significant increase in cyber defense across the board.

In conclusion the key takeaways from this Cyber defense strategy Pillar is the need to be able to find and eliminate cyber threats before they are able to occur, the

ability to for high degree of teamwork amongst a collations of different agencies and companies, the disrupt cyber criminals and adversary nation's ability to fund and gather resources necessary to launch cyber attacks against the nations. These four key elements of this pillar are what I believe to be the most important aspect of this particular Pillar.

SOURCES

President Biden. (2024). *NATIONAL CYBERSECURITY STRATEGY*

IMPLEMENTATION PLAN VERSION 2.

https://www.whitehouse.gov/wp-content/uploads/2024/05/National-Cybersecurity-

Strategy-Implementation-Plan-Version-2.pdf