

Ethical Implications of The National Cybersecurity Strategy of the United States

Brandon Zachary Pearson

Old Dominion University

CYSE425W - CYBER STRATEGY AND POLICY

Professor Malik A. Gladden

December 9, 2023

Cyberattacks have become a major threat to the United States and many other countries. This has led to many concerns about what will be done in order to address such threats. The United States is addressing these concerns by implementing The National Cybersecurity Strategy. The National Cybersecurity Strategy of the United States is a complex strategy that will take the collaboration of many entities. The major discerning goal of this strategy is to protect the nation's critical infrastructure. Just like many other government plans there is controversy behind them and concerns about how it will be implemented. Additionally, there are concerns when it comes to regulations and policies that come with this strategy. Primarily, focusing on ethical issues that could arise if the government oversteps people's rights in order to achieve the goal they have set out. Concerns on how far the government will go to ensure that the nation is deemed protected. One thing that needs to be kept in mind when implementing this strategy is balancing individual rights with the potential good that this strategy could achieve. Just like many other strategies the good needs to outweigh the potential loss of privacy or limits it places on one's rights.

When looking at this strategy it is attempting to create an overall safer cyberspace. This is a complex task to achieve without potentially redistricting individuals' rights. The strategy is attempting to achieve these goals by approaching them through collaboration. At the same time, it may cost some level of individual rights or place more restrictions and policies surrounding cybersecurity. It is out of attempting to protect the nation. The issue that many take upon with such infringement on individuals' privacy is it could mean that the government will be able to monitor what they are doing. This has been a concern of individuals for years now. "In the United States, for example, the Communications Assistance for Law Enforcement Act of 1994 requires telecommunications providers to build their networks in ways that make government

surveillance and interception of electronic communications possible.” (Richards, 1941). The government may be going too far with potential surveillance and data collection programs. From the government's perspective, these programs allow them to detect threats at a greater rate, allowing them to dismantle threat actors and prevent attacks from happening. This ends up having a positive effect because it is protecting the nation. “The balance between security and privacy must be struck carefully, and the use of surveillance technology must be justified as necessary and proportional to the threat. Additionally, citizens must be informed and have their privacy rights respected.” (Gondek). The main thing that should be done is trying to find a balance between respecting the rights of the people while at the same time creating effective solutions to mitigating attacks.

One counterclaim that can be made is that there is already a wide range of surveillance technologies being used that people don't pay any attention to. This can be apps and features on their phones that collect data on users. Yet, more often than not users blindly accept such features without understanding the data they are giving up. The only time people make a commotion about it is when the government is the one doing it or implementing such programs. Additionally, one concern is that the government could use such programs with the intent to protect the nation from cyberattacks, but they could also use those programs for things that aren't related to the initial goal.

When looking at the National Cybersecurity Strategy it is clear that it is setting out to achieve something that will positively impact the nation. Ensuring that the nation is better addressing cyberattacks and imposing new regulations to ensure corporations are doing the same. The issue that presents itself is ensuring that the steps taken to reach the goal are ethical and don't overstep individuals' rights. This is no easy task and never has been an easy thing to do. No

matter what type of policy, regulation, or strategy that comes about it has to be done tactfully.

This must be done to ensure that the implementation of them is done in a balanced way.

Balancing the good that it brings with the potential negative side effects it also may impose.

References

Gondek, Christopher. "Privacy vs. Security - Striking the Right Balance." OriginStamp, originstamp.com/blog/privacy-vs-security-striking-the-right-balance/. Accessed 09 Dec. 2023.

National Cyber Workforce and Education Strategy - the White House, www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

Richards, Neil M. The Dangers of Surveillance, cordellinstitute.wustl.edu/wp-content/uploads/2020/11/Dangers-of-Surveillance-Richards.pdf.