EFFECTIVE RESPONSE MEASURES FOR THE UNITED STATES AGAINST CYBER ATTACKS CONDUCTED BY STATE ACTORS

BY: BRYANT WATKINS

4/5/2025

CYSE 425W

Prof. Bora Aslan

Cybersecurity and relevant policies have far reaching implications for all aspects of life. A major aspect that many often do not consider would be the implications for society. The development of any cybersecurity policy or strategy often has influence from a plethora of social factors. Cyber policies will also have certain consequences that will affect society. Ultimately, cybersecurity policies can be drastically shaped by cultural and subcultural influences.

Two major factors from society that influences this specific policy are trust and societal sustainability. The United States government has always tried to establish a sense of trust amongst its citizens. One way to establish trust from your citizens is to maintain a cyber policy that allows them to feel safe, doing so lets them know that you will defend them as well as their data and assets. This policy does just that, as strong counter attack measures on adversarial nation states will prove to be a strong deterance. In the absence of attacks from foreign adversaries – American citizens will have more trust in the government's ability to safeguard their interests.

Societal sustainability is another area of major influence on this policy. "Without cybersecurity, the sustainability of our modern, digitalized society is at risk" (Maigret, 2023). Society cannot possibly be sustained in the presence of debilitating attacks on cyber infrastructure by adversaries. This policy works to prevent and detere this possible attacks. Without the fear of utilizing cyber infrastructure, society will have confidence in their ability to conduct tasks such as submitting payments digitally or having their data stored digitally.

This policy will certainly have some consequences for society as well. One major consequence could be the potential for surveillance, which some may view as government overreach. Surveillance and government observance have historically been an area of concern for many Americans. The government request for access to the phones of the San Bernadino

shooting suspects in 2016 is a prime example, a Pew Research Center survey at the time found that while a majority of Americans sided with the FBI – a considerable amount did not (Olmstead & Smith, 2016). This policy very well may require the government to observe or conduct surveillance on American citizens, specifically if the government suspects certain citizens of colluding with foreign adversaries in conducting attacks on the United States.

Another potential consequence for society under this policy could be the restriction on using foreign technologies or systems. An example for this is the ongoing debate on American citizens using the app Tik Tok. A major argument against such use is the potential for American adversary China to collect data on America, data that could be used to conduct attacks on cyber infrastructure in the United States through something such as theft. If China were to conduct a cyber attack on the United States, then this policy could entail the restricting the use of Chinese systems and technologies by American citizens as one aspect of an effective response measure.

Cultural and subcultural influences have absolutely shaped this policy. One way is that American culture has increasingly entailed the proliferation of technology in our society. Technology has increasingly been used in many aspects of societal culture, from more payment card readers to more biometrics in establishing forms of security. Given the great increase in technology prevalance – society has seen an increasing need for a secure technology space (Creese, Dutton & Esteve-González, 2021). “As the percentage of the world’s population using the Internet for more significant activities has grown, so has the interest in building a secure cyber space” (Creese, Dutton & Esteve-González, 2021). This policy has been designed to instill a sense of security of American infrastructure and interests as a result of this cultural influence.

America also has a culture of believing in the protection of many rights, as seen with the occasional national protests and lawsuits that pertain to the belief that a certain right is being

violated. This cultural influence shapes this policy by creating its determination to safeguard the right to privacy and security for all citizens. Mitigating cyber attacks is one thing – but this policy seeks out counter measures that further enhance the protection of American rights and facilitate a secure cyber space. The totatlity of all such factors has ultimately shaped the social implications for this policy.

REFERENCES

Maigret, B. (2023). Cybersecurity: A Necessity for the Sustainability of Society. In - *society#:~:text=A Lack of Cybersecurity Puts Society at Risk&text=When a cyberattack targets these,and business stability and continuity*.

Olmstead, K., & Smith, A. (2017). Attitudes about Cybersecurity Policy. *Pew Research Center*, *3*.

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and Ubiquitous Computing*, *25*(5), 941–955. doi:10.1007/s00779-021-01569-6