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

BY: BRYANT WATKINS

MARCH 7, 2025

CYSE 425W

Professor Bora Aslan

Policy in the United States is crafted by lawmakers, so there are sure to be political implications with any major cyber policy. The United States, unlike most other nations, is dominated by two major political parties – Democratic party and Republican Party. Both political parties have addressed the cyber policy proposed. There is a plethora of factors that have led each respective party to the manner in which they addressed said policy. The manner in both parties addressed said policy ultimately comes with ramifications from the not only the American public but the world as well.

The development of state cyber policy and actions has transformed society forever and created some divisions amongst political factions (Kormych & Zavhorodnia, 2023). Some political factions believe that the federal government has overstepped its boundaries for cyber operations, especially as it pertains to surveillance. Surveillance ramped up considerably following the September 11, 2001 attacks. Republicans have grown more skeptical of defensive surveillance efforts in recent years, increasingly since the Russian 2016 election meddling incident (Merchant & Fingerhut, 2023).

Though there have been recent shifts in views on national defensive operations politically in the United States – historically the Republican party has been perceived as being more "hawkish" on U.S defensive operations abroad. So hypothetically the Republican party would be highly supportive of cyber defensive, but both parties are known to be relatively equally supportive of conducting responsive military operations when the United States has come under attack. The United States cyberspace and military began becoming interconnected in the 1990's, which eventually culminated in the Pentagon adding the cyberspace as the fifth dimension of warfare (Cavelty & Wenger, 2019).

United States politicians have addressed this policy by passing legislation strengthening the powers and authority of the federal government to safeguard its citizens and infrastructure. This can directly be seen with the passage of the Strengthening American Cybersecurity Act of 2022. This legislation crafted by political lawmakers further empowers the federal government to combat and conduct defensive cyberoperation responses to threats by any adversarial actor – including other nations or states. This legislation was a groundbreaking development in the cyberspace of the United States, arguably something in the political landscape that is the most consequential since the Stuxnet attack against Iran.

Lawmakers ultimately reached such conclusions leading to said legislation due to ever expanding threat landscape the United States cyberspace infrastructure faces, especially from state actors. International adversaries have essentially turned to ‘”netwar’” following the cold war era heading into the 1990’s (Beyer, 2023). The modern-day military landscape is much more than physical fighting on battlefields – it is now increasingly fought in the cyberspace. American legislators and political figures have come to such a realization. Ensuring the security of the American people and infrastructure now requires significant considerations for the cyberspace, leading to the development and deployment of defensive cyberoperations.

There are of course major ramifications of these policy makers’ decisions. Going back to 2010/2011 – the Stuxnet attack, conducted by the United States and Israel, ushered in a new era of the international cyberspace. The posturing of U.S politicians to target adversaries by means of the cyberspace has led to a steady increase of other nation states conducting their own international cyberoperations. We have seen numerous international cyber incidents – Russian cyberattack on Estonia, China’s Operation Auroa, North Korean Sony hack, and Russian 2016 election meddling to name aa few. Americans have also grown weary of surveillance aspects of

U.S cyberoperations, as well as engaging in further escalatory conflicts overseas. All of these ramifications are assuredly major concerns that must not only be taken into consideration by U.S policy makers – but the world as well for the foreseeable future.

REFERENCES

Kormych, L., & Zavhorodnia, Y. (2023). The concept of modern political confrontation in cyber space. *Journal of Cybersecurity*, *9*(1). doi:10.1093/cybsec/tyad017

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Beyer, J. L. (2023). The Politics of Cybersecurity and the Global Internet. *Perspectives on Politics*, *21*(2), 664–668. doi:10.1017/S1537592723000361

Fingerhut, H., & Merchant, N. (2023, September 21). *Democrats and Republicans are skeptical of US spying practices, an AP-Norc Poll finds*. AP News. https://apnews.com/article/intelligence-section-702-apnorc-poll-4ef1e9f300395d0d7cda5b86cf7d5785