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

BY: BRYANT WATKINS

FEBRUARY 14, 2025

CYSE 425W

Professor Bora Aslan

The policy of effective response measures for the United States against cyber-attacks conducted by state actors is rooted in safeguarding national security interests and infrastructure of the United States. The collective defense of a nation is not simply rooted in physical warfare, the cyberspace in the modern day is another critical pillar of society that requires a secure environment. Securing this environment on the behalf of a nation is the duty of said nation, in this case that is the duty of the United States to achieve. A major step in achieving this is to set out a clearly defined policy addressing grave cyber threats.

There are three factors that led to the need of this such policy – the sheer evolution of technology, previous instances of cyber incidents involving state actors against the United States, and an increase in the interconnected nature of technology. Technology since its inception has taken leaps and bounds, so has the knowledge of it and various threats it faces or poses. Technology over time has also become far more interconnected over time (Quinn, 2023). This interconnectivity of course involves not only allies – but adversaries as well, and so it is expected to receive attempts of cyberattacks from state actors from time to time. There have already been numerous attacks against the United States by state actors conducted through cyber means, two prominent instances include – Iran's DDoS attack in 2012, and Russia's election meddling of 2016 (Boyte, 2017; Bossetta, 2018).

There are numerous steps to applying this policy in a specific setting. Step one of course involves first mitigating the attack – possibly by disconnecting computer networks from the World Wide Web and coordinating with cybersecurity professionals nationally, as well as internationally with allies, to block relevant unique IP addresses (Boyte, 2017). Step two entails tracing the digital signatures back to its origin as to identify the guilty party (Boyte, 2017). Step three is to then gather intelligence on said guilty party, likely again with the assistance of

international allies. Step four, once all available intelligence has been gathered – then this intelligence must be discussed amongst a close circle of high-level United States defense officials in coordination with cybersecurity experts to consider appropriate actions (i.e sanctions, possible military action, cyberattacks, etc.). The final step, once appropriate action is recommended – it is then brought to the President or U.S congress to approve depending upon its scale.

There are also a couple of highly effective preventative measures to consider as well. Considering that many attacks are conducted through a surge in traffic, as seen with the 2012 attack, then U.S network administrators should be well trained in quickly identifying and blocking abnormal spikes in traffic (Boyte, 2017). The United States should refrain from utilizing any equipment or software known to originate in adversarial nations (Boyte, 2017). By using assets originating in adversarial nations – the United States increases its risk of said state actor conducting attacks against its cyberinfrastructure. These are two of the most effective means to prevent cyberattacks from state actors preemptively and proactively.

This policy overall fits seamlessly into a broader national policy. The United States has had national defense policies dating back to its inception. With the United States' defense policy has always come along a response posturing that is tailored to addressing certain threats in the interest of safeguarding the United States. The President, Department of Defense, Military, and Congress are always planning for military response considerations in case of physical warfare – this policy discussed is simply an additional consideration of cyber warfare. Some common defense response measures include – deployment of troops, missile strikes, drone strikes, blockades, etc. Inclusion of this discussed cyber policy would add additional options such as – sanctions, surveillance, cyberattacks, etc. Given the potential for escalation into broader conflict

– the final approval is still vested with the President or U.S congress, as with other typical physical means of defensive military operations against other nation states.

WORK CITED

Boyte, K. J. (2017). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. *International Journal of Cyber Warfare and Terrorism*, *7*(2), 54–69. https://doi.org/10.4018/IJCWT.2017040104

Quinn, T. P. (2023). *An Assessment of the U.S.' Preparedness for Foreign Cybersecurity Threats*. ProQuest Dissertations & Theses.

Bossetta, M. (2018). THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY. *Journal of International Affairs*, *71*(1.5), 97–106. https://www.jstor.org/stable/26508123