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

BY: BRYANT WATKINS

MARCH 28, 2025

CYSE 425W

Professor Bora Aslan

This cyber policy deals with the issue of attacks by other nation states, as well as the cyber means by which the United States may respond and defend itself – essentially cyber warfare. There are numerous ethical considerations for the realm of cyber warfare, much like there are for traditional military warfare. The relevant ethical considerations are most consequential for the civilian population of any nation state. While the goal for any cyberattack against an actor may be to inflict debilitating damage – civilians being caught in the crossfire is typically frowned upon. Additional considerations will range from cost and benefits to individuals' rights.

The assets and personnel for cybersecurity can be incredibly expensive, especially when on the scale needed for nations to engage in international affairs. Ultimately, the United States congress is the one who controls the purse for the Department of Defense budget. The costs are a relatively straightforward prospect for this policy, but the benefits are another matter. The benefits of this policy are nearly incalculable, there are a plethora of factors that may influence this. A major benefit of this policy is the prevention or mitigation of potentially devastating cyber attacks that may cause billions in damages and data loss. Another major benefit of this policy is the further enhancement of national security – something you cannot necessarily put a price on, but is certain to increase the confidence of the American people in their government.

The types of rights that are protected and potentially limited with this policy is a much more complex matter. "Criteria are needed to determine proportional responses, as well as to set clear thresholds or 'red lines' for distinguishing legal and illegal cyberattacks, and to apply appropriate sanctions for illegal acts" (Floridi & Taddeo, 2018). The lines are incredibly blurry as it pertains to the rights of actors and nations in conducting cyber attacks against adversaries.

There are no concrete rules of engagement on the international scale in cyber warfare like there are with traditional warfare.

Nations are permitted the right to defend themselves against malicious cyber-attacks by other actors, but there are also limitations on those rights. Under international law – there are certain "criteria for identifying crucial national infrastructures, such as health systems or key energy and water supplies that should be protected" (Floridi & Taddeo, 2018). Cyber defense measures that branch out into the physical realm, such as attacking hospital systems causing the disabling of certain medical equipment necessary for patient care, could very well be seen as war crimes. It is imperative that while nations exercise their right to defend their national security and sovereignty – they also abide by limitations to these rights as it pertains to civilians and critical infrastructure.

This policy will also need to address individuals' rights. The issue of privacy versus security is a balancing act that will likely never be adequate for all. "Militaries in democratic states are not afforded blanket exemptions from upholding privacy" (Hempson-Jones, 2018). Not only is it important not to infringe upon the rights of native citizens – but citizens of other countries as well. Spying and surveillance is typically the biggest culprit of individuals' rights being violated. United States congress does have laws in place to protect against unwarranted surveillance but internationally is a separate matter. International matters often cause conflicting concerns amongst nations, one may feel the right to spy on a suspect and the other nation may feel that this is a violation of said individual's rights.

This policy will ultimately address individual rights appropriately due to existing U.S law(s). These laws may be de jure legislation such as the Cybersecurity Information Sharing Act of 2015, or "soft" laws such as executive orders or internal policies (Margulies, 2017). The

United States Department of Defense has existing criteria on the books for apprehending or spying on international criminals and suspects, so cyber operations such as surveillance will exist under said existing criteria – regardless of the protest of other nations. The United States has a duty to protect its national security interests, and sometimes that just may come into conflict with cyber affairs of other nations.

References

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature, 556*(7701), 296-298. https://doi.org/10.1038/d41586-018-04602-6

Hempson-Jones, J. S. (2018). The Ethics of Online Military Information Activities. *Journal of Military Ethics*, *17*(4), 211–223. https://doi-org.proxy.lib.odu.edu/10.1080/15027570.2019.1586357

Margulies, P. (2017). Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. *Indiana Journal of Global Legal Studies*, *24*(2), 459–496. https://doi.org/10.2979/indjglolegstu.24.2.0459