Policy Analysis Paper 1 - CYSE 425W

Jaden Lewis

Bora Aslan

CYSE 425W

2/16/2025

Introduction

With the introduction of technology itself and advancements in this technology, cyber threats are bound to become increasingly more sophisticated and common. Digital self-defense (hacking back), has emerged as a possibly beneficial strategy to counter these malicious hackers. This strategy has become a bit of an ethical dilemma as some believe for this to be a necessary action against cybercrime, where others believe it's a thin line between defense and crime. This paper will explore the ethical dilemma of digital self-defense, scenarios where this strategy may be necessary, and the practicality of using this strategy today.

Is hacking back ethical?

Whether or not hacking back is ethical depends on the execution. One of the biggest potential dangers with hacking back is counter-strikers accidentally hitting innocent third parties rather than the actual hacker, as it's very easy to conceal the real source of the attack (Majuca & Kesan, 2009). One of the main reasons as to why cyber attacks are so dangerous and difficult to solve is because an attack, in the right hands, can be nearly untraceable. It's not uncommon for organizations to repeatedly be led to the wrong target when trying to pinpoint the source of an attack. Another potential danger with hacking back is the risk of escalation. It's a real possibility that instead of deterring cyber attackers, hacking back may instead urge the hackers to counterattack stronger against more valuable systems (Iasiello, 2014). This may also give the hacker information as to the limits and capabilities of the defender, as well as what tools they may be in possession of. Lastly, there is the risk of friendly fire. Let's look at it from a government's perspective, what would happen if the attackers operated from an allied or friendly country? Can a government legally attack the infrastructure of allied or third-party nations

without the consent of the host government? (Iasiello, 2024). This would likely lead into much bigger problems between two nations. I believe that digital self-defense (hacking back) can be ethical when dealing with very specific scenarios but is also something that is risky if not properly executed.

When hacking back is necessary

Hacking back can be necessary to empower private sector organizations to "take a more active approach to their cyber defense" (Review, 2021). It's not a surprise that organizations may feel that passive security is not enough. The usual response to a cyber attack is to identify how it happens, collect information on compromised data, and implement measures to prevent or minimize damage. The problem with this is that it does not prevent future attacks from happening, it only strengthens your protection toward future attacks, yet inevitably this will happen again, and these responses will be repeated again. If hackers are aware that honeypots, sandboxes or beacons are used by the defender then they could possibly reversive engineer the defensive software or circumvent that software (Philippe Martens, 2021). Whether or not hacking back is necessary or not ultimately comes down to the law, although I personally believe for it to be unnecessary as there are other methods that are much more effective against cyber attacks.

The practicality of hacking back

Research shows that hacking back is not only rarely necessary, but causes more harm than good. The biggest reason being that it may invite more attacks as a counter, but also because it's much less practical than other methods of cyber security. One method being, the use of a "honeypot". This refers to organizations having a mirror network to lure attacks to target first,

through which defenders can monitor techniques and apply defensive strategies to their organizations true networds (Iasiello, 2014). This allows for a more legal/ethical process of defending against cyber crime while still being able to monitor the attackers and develop ways to further increase security. Since hacking back requires so many variables and specifics it is currently not very effective against deterring cyber attacks. This is subject to change in the future but as for today this strategy is not very practical in cyber security.

Conclusion

In conclusion, digital self-defense (hacking back) is a very controversial subject in the world of cybersecurity. Some believe that it's necessary to prevent future attacks while others, the majority, believe it to be an enabler for further, stronger cyber attacks. From the evidence listed above we can conclude that this strategy of digital self-defense is not the most effective, practical method of deterring cyber attacks today, but may become more effective in the future as we continue to make advancements in technology and cyber security.

References

Majuca, R. P., & Kesan, J. P. (2009). Hacking Back: Optimal Use of Self-Defense in Cyberspace. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1363932

Iasiello, E. (2014). Hacking Back: Not the right Solution Hacking Back: Not the right Solution. Article, 44, 9–10. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2732&context=parameters

Review, L. (2021, January 16). The “Hack Back” Bill: A Necessary Defense Mechanism, or a Precipitous Disaster? Wake Forest Law Review. https://www.wakeforestlawreview.com/2021/01/the-hack-back-bill-a-necessary-defense-mechanism-or-a-precipitous-disaster/

Philippe Martens (2021). Self-defense in Cyberspace: Hacking Back the Hacker. Tilburg University. https://arno.uvt.nl/show.cgi?fid=155524