Digital Self-Defense (Hacking Back)

Policy Analysis Paper 3

Kristofer Vargas

CYSE 425W

Old Dominion University

Though it was once a place of wonder and discovery, the inevitable shortcomings of human nature have infected the Internet and the digital world as a whole. Because of this, criminals and malicious beings are somewhat commonplace online, and prey on the vulnerable in order to gain access to their personal information. To fight and counter these predators, the concept of "hacking back" has been brought up in political spheres as a form of digital self-defense. This would entail individuals and the private sector taking initiative and tracking down the perpetrators post-attack. Zeroing in on the responsible parties would allow for any data stolen to be recovered and the systems of the hackers to be disabled before further malicious activity occurs. On paper, this seems to be a no-brainer, as those who are capable of swift and professional retaliation would be able to counter their attackers, leading to the apprehending of dangerous individuals, akin to the work of a vigilante superhero supporting law enforcement. However, the concept of "hacking back" arouses many problems and issues that have contributed to it not currently being recognized as a legal form of action for individuals or private sector companies to take. Among these issues, there are believed to ethical shortcomings that make "hacking back" an immoral activity that would cause more damage than benefit to those involved.

The first ethical implication is the issue that "hacking back" presents a form of vigilantism that undermines the workings of the law. The main right of citizens that this could apply to would be the right to self-defense in the occurrence of a threat or violence from another party. Relating this to "hacking back" and digital self-defense, the same principles could be applied on a technological scale. The hackers that have attacked and stolen sensitive information are undoubtedly an apparent threat and though the danger posed is not in a physical sense, the consequences posed by malicious acts such as identity theft or fraud are very real and

devastating to the victimized party. Engaging in counterattacks such as “hacking back” can be seen as a form of self-defense that is supported by the right for individuals to seek to protect themselves from imminent threats. When it comes to the rights that are being compromised by the policy, these would be the rights of the perpetrators. Though the criminals that engage in cyberattacks on the weak are villains that trample all over the ethics involved with Internet privacy, they are still technically entitled to their own privacy. Choosing to bypass the rights of the criminals could be interpreted as selective governance and would jeopardize the overall legitimacy of the law.

The second glaring ethical implication is the shortcoming of “hacking back” is the potential for escalation that can lead to large-scale conflicts and collateral damage. Should the act of counter hacking be engaged in and performed adequately, there is no surefire way to mark this as the end of the conflict. Even if the perpetrators are identified and disabled, they could still find avenues of launching yet another attack in retaliation towards the original victims or even close associates of the victims, dragging more innocents into the crossfire. In this case, the situation would eventually spiral out of control, as attacks and counterattacks are leveled by each side and more and more innocent people fall victim to collateral damage. These damages could very easily add up to large financial repercussions and the loss of privacy for individuals that had nothing to do with the original conflict in the first place. The involvement of innocents and the losses they would suffer are poignant examples of immorality and an ethical issue that would stand in the way of “hacking back” being a widespread solution to cyberattacks.

When taking an overall look at the way in which the policy of “hacking back” addresses the issue of individual rights, this is probably one of the main roadblocks in the way of the policy ever being fully implemented into legislation. The individuals rights to privacy and self-defense

that support the victims engaging in “hacking back” are the same rights that are being limited on the side of the criminals and perpetrators. When it comes to law and order, selective treatment based on the roles of the parties involved would be hard to apply to the situation without somewhat undermining the regulations put into place. Being able to engage in digital self-defense is an example of exercising the individual’s right to self-defense, but in doing so, the retribution of the opposing party would be somewhat justified under the law. The criminals technically also have the personal right to privacy and engaging in their own form of self-defense, which just leads to an unbridled mess of chaos. With how vague and blurred the ethical lines are when it comes to “hacking back”, steps towards implementing the policy as an official law are not currently plausible without clear and concise ethical guidelines being put in place by a governing body as to what is allowed when “hacking back” and the specific individual rights that get forfeited once a party has been identified as a malicious actor.

Sources Cited:

Steinmetz, K., & Gerber, J. (2014). “It Doesn’t Have to Be This Way”: Hacker Perspectives on Privacy. *Social Justice, 41*(3 (137)), 29–51. http://www.jstor.org/stable/24361631

Holzer, C. T., & Lerums, J. E. (2016, May). The ethics of hacking back. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). IEEE.

Lin, P. (2016). Ethics of Hacking Back: Six arguments from armed conflict to zombies. *Available at SSRN 4682398*.

Himma, K. E. (2008). Ethical issues involving computer security: hacking, hacktivism, and counterhacking. *The handbook of information and computer ethics*, 191-217.

Ethical and legal aspects of hacking back. Blue Goat Cyber. (2024, February 14). https://bluegoatcyber.com/blog/ethical-and-legal-aspects-of-hacking-back/#:~:text=The%20Morality%20of%20Retaliatory%20Hacking&text=However%2C%20opponents%20contend%20that%20hacking,collateral%20damage%20cannot%20be%20ignored.

The hack back: The legality of retaliatory hacking. Pulse. (n.d.). https://www.allens.com.au/insights-news/insights/2018/10/pulse-the-hack-back-the-legality-of-retaliatory-hacking/#:~:text=Dr%20Alana%20Maurushat%20advocates%20for,harm%20sustained%20by%20the%20victim.

Maclean, D. (2018, May 30). *The problems with hacking back.* AFCEA International. https://www.afcea.org/signal-media/problems-hacking-back

Winstead, N. (2020, June 26). *Hack-back: Toward a legal framework for Cyber Self-Defense*. American University. https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm#:~:text=The%20rights%20of%20private%20entities,the%20role%20of%20the%20state.