Digital Self-Defense (Hacking Back)

Policy Analysis Paper 2

Kristofer Vargas

CYSE 425W

Old Dominion University

With the current dangers that are presented by digital threats such as hackers and cybercriminals, it is paramount that the practice of digital self-defense becomes more commonplace. Digital self-defense encapsulates the different strategies and practices that can be taken up in order to better protect oneself from the different pitfalls presented by Internet predators. But to take this even a step further, a more specific branch of digital self-defense, known as “hacking back”, characterizes the use of offensive hacking maneuvers by the victimized party in order to disable or recollect any evidence or resources that have been stolen. This particular issue has come under the political microscope in recent years, as there have been advocates of the idea have voiced their support for a policy to be put into place that cements its legality. But even with this growing support system, there are still some that oppose the proposed policy, as there are questions surrounding how Internet governance could be jeopardized and the “wild west” that the cyber landscape could morph into should hackers and victims engage in cyber shootouts.

With current standings regarding legislation that deals with online privacy and regulating cybercrime, there are restrictions in place that hold back victims from being able to exact their own forms of offensive hacking as revenge. It is currently illegal for victims to launch counterattacks against their perpetrators in order to minimize the ability for the criminal party to engage in malicious activity with data gained through unauthorized access or disable the systems of the guilty party. Because of this, victims that are somewhat capable of taking matters into their own hands are left to wander aimlessly until official cyberspace regulating bodies come to their rescue. In this downtime, the criminals can engage in countless forms of cybercrime with their newly stolen information, such as fraud and identity theft. This can often lead to large financial consequences, as well as deteriorating the mental well-being of the victimized party due to the stress that these situations can cause. The solution to these troubles would be to develop and instill a cybersecurity policy that not only legalizes but encourages the right to digital self-defense and "hacking back". The implementation of this policy would give way to numerous political implications, but the main ones would be limits on Internet governance and enhancing the overall abilities of the private sector.

Given the involvement of the private sector into the issue of hacking back, there have been a handful of policy makers that have voiced their relative interest regarding the policy. These include some that are in favor of legalizing the right of the private sector to freely operate in digital defense, and others that view the legalization as bearing too many potential risks. One of the biggest and most active proponents of a digital self-defense policy was lawmaker Tom Graves, who served in the U.S. House of Representatives for Georgia's 14th district from 2013 to 2020. Graves proposed legislation known as the Active Cyber Defense Certainty Act (ACDC), which would attempt to bypass restrictions put into place by the CFAA. The CFAA was enacted in 1986 and acts to put criminal punishments and penalties into place for people that bypass protections of computers and engage in unauthorized access in order to access sensitive information systems. The ACDC would have taken these measures and throw them by the wayside, by legalizing the ability for both individuals and the private sector to utilize hacking tools in order to track down attackers and potential criminals before they can even attack. However, the detractors of this policy that contributed to ACDC's inability to get passed into law have cited numerous issues with hacking back, namely the "chaotic environment" that legalized hacking would create, the abilities of hackers to pin responsibility onto innocent parties, and the alternative of strengthening defensive capabilities instead of legalizing hacking back. Elsewhere on the political landscape, two more individuals that sought out the potential of this policy coming to fruition were the Senators Steve Daines and Sheldon Whitehouse, representing Montana and Rhode Island respectively. Daines and Whitehouse worked together to propose a bill that would call upon the Department of Homeland Security to look into the potential of allowing the private sector to engage in "hacking back" in order to fend off cyberattacks. To do so, the bill (much like the proposed ACDC by Graves) would alter the restrictions put into place by the CFAA in order to give leeway towards private companies and their ability to respond to targeted attacks. For much of the same reasoning as the ACDC, the Study on Cyber-Attack Response Options Act was not fully voted into law, as many still saw drawbacks regarding the ability for hackers to disguise who was ultimately the responsible party leading to mistakes by the retaliating parties and the potential for unintended damages.

Due to failure for any solidified policy to be made regarding digital self-defense and "hacking back", there is still uncertainty surrounding the potential for individuals and private sector companies to engage in counterattacks. Within the political landscape, the efforts of figures such as Graves, Daines and Whitehouse gained some attention and traction, but ultimately fell short regarding how much steam they could pick up. There is still too much concern about the wild goose chase that hackers would lead counterattack on, meaning that innocent parties would be pinned as criminals and the collateral damages would begin to add up. Perhaps at some point in the future, the idea of "hacking back" may become a more plausible policy change if the general public begins to get more educated and informed regarding the ins and outs of ethical hacking. But as things currently stand, "hacking back" will have to be placed on the metaphorical back burner due to its risks involved that would create a digital battlefield that would be nearly impossible to regulate.

Sources Cited:

O'Connor, N., Lange, A., & Lange, A. (2015). Privacy in the Digital Age. *Great Decisions*, 17–28. http://www.jstor.org/stable/44214790

Norman, L., & Beckman, L. (2024). Democratic self-defense and public sphere institutions. *Constellations*.

Thibodeaux, A. (2015). *Hacking back: Surviving in the digital age* (Master's thesis, Utica College).

Couzigou, I. (2020). Hacking-back by private companies and the rule of law. *Heidelberg Journal of International Law*.

Sheldon, R., & Cole, B. (2023, August 1). *What is the Computer Fraud and abuse act (CFAA)?: Definition from TechTarget*. Search Security. https://www.techtarget.com/searchsecurity/definition/Computer-Fraud-and-Abuse-Act-CFAA#:~:text=The%20Computer%20Fraud%20and%20Abuse%20Act%20(CFAA)%20of%201986%20is,whose%20access%20exceeds%20their%20authorization.

Vavra, S. (2019, June 13). *Congress to take another stab at "hack back" legislation*. CyberScoop. https://cyberscoop.com/hack-back-bill-tom-graves-offensive-cybersecurity/

Williams, B. D. (2024, March 4). *Proposed "hack-back" Bill tells DHS to study allowing companies to retaliate*. Breaking Defense. https://breakingdefense.com/2021/07/proposed-hack-back-bill-tells-dhs-to-study-allowing-companies-to-retaliate/

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.