Digital Self-Defense (Hacking Back)

Policy Analysis Paper 4

Kristofer Vargas

CYSE 425W

Old Dominion University

As the scope of influence regarding the cyber realm has continued to expand, society has become increasingly involved in any and all matters taking place in the digital world. Of these matters, the issues regarding the ins and outs of cyber-attacks and defense, what is allowed, and what is socially acceptable has been discussed at length. In particular, a policy that has been discussed often is digital self-defense or "hacking back". This policy centers around hacking as a form of retaliation, and victimized companies/businesses being given the green light to pursue their attackers in order to regain any lost evidence or shut down their systems. On the surface, this policy may seem like a no-brainer to some, as the United States prides itself on the ability of citizens to engage in self-defense should they be targeted or feel threatened. Having this same line of thought applied to the digital world would mean that engaging in hacking back is simply defending one's property. But in the current state of things, hacking back is still seen as a controversial policy idea and has many detractors.

Of the key social factors that have led to the development of this policy, the increase in social issues involving the right to self-defense can be accredited heavily. In recent years, the second amendment of the United States Constitution has been used in arguments to either justify or criticize people's actions. This amendment serves to solidify the right of people to bear arms and have a means of self-defense and protection. This pertains to the living world but has yet to cast its influence in the digital world. When it comes to cybercrime, there is currently no set policy or law in place that allows for self-defense to be legally conducted. Due to this, cybercriminals are more prominent and harder to track down sometimes compared to your everyday bank robber. Digital traces are fainter, and hackers evolve their techniques constantly, leaving cybersecurity specialists to constantly pursue them. The solution to this wild goose chase has led some to suggest that digital self-defense be made legal and socially acceptable. When it comes to the social impact that the policy of hacking back would make, the wide majority of them appear to be generally negative. Hacking back is seen by most to be more akin to vigilantism than formal police work. Giving private sector entities and business the freedom to engage in the own line of hacking, even if for good reason, could lead to widespread escalation. This would result in a back-and-forth war of retaliation taking place between hackers and private sector entities, with each cyberattack being larger and more damaging than the last.

Should hacking back be made into formal legislation and no longer just a policy idea, there are a plethora of immediate social implications that would sprout up and affect everyone. Besides the previously mentioned issue of escalation, the second big social implication would be the birth of heavy weaponization by digital means. This application works hand in hand with the issue of escalation, as the heightened frequency of attacks being mounted by both perpetrators and defenders would incentivize both sides to increase their abilities. In turn, a sort of "arms race" would commence, in which the attacks would become larger in scale, include increasingly malicious agents, and inadvertently affect more innocent people. Is it well-documented that hacking back is no small feat in the world of cybersecurity, and only very high-level professionals with considerable technical expertise will be able to pull it off without any unintended collateral damage. If hacking back was to be made into a legal practice, chances are that a large percentage of the people engaging in it would not meet these requirements. Consequently, large numbers of civilians would face repercussions for a conflict that they are not directly involved in, and these damages would amount to large fines and penalties having to be dished out.

Hacking back is a very unique practice and concept, so it must not be directly correlated to real-life self-defense like many of its proponents wish to do. The digital realm as a whole is a different playing field and boasts different consequences that need to be considered. So as things currently stand, the negative social implications of hacking back are classic warning signs that suggests that it should stay as a mere policy idea for the time being. If there are significant strides made in terms of figuring out how it will be regulated and strict rules are put into place for the private sector entities to follow, then maybe the policy will be able to become socially accepted and a full-fledged piece of legislation in the future.

References:

Kilger, M. (2017). ANTICIPATING THE NATURE AND LIKELIHOOD OF A CYBERTERROR COMMUNITY. In T. Saadawi & J. D. Colwell (Eds.), *CYBER INFRASTRUCTURE PROTECTION VOLUME III* (pp. 157–192). Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep11978.10

Lemay, A., & Leblanc, S. (2021, June). Is Hacking Back Ever Worth it?. In *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (p. 239). Academic Conferences Inter Ltd.

Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. *Social Science Computer Review*, *23*(1), 8-23.

Mancino, T. H. (2015). Hacking Back: Active Cyber Defense. In L. D. Miller (Ed.), *The Army War College Review* (pp. 42–46). Strategic Studies Institute, US Army War College. http://www.jstor.org/stable/resrep11941.6

Ellis, J. (2024, January 24). *Cyber hack back is still wack: Rapid7 blog*. Rapid7. https://www.rapid7.com/blog/post/2021/08/10/hack-back-is-still-wack/#:~:text=Not%20only%20should%20this%20concern,can%20spot%20and%20stop%20abuses.

Lin, P. (2024, January 26). *Ethics of hacking back: Six arguments from armed conflict to Zombies*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4682398#:~:text=Abstract,more%20carefully%20consider%20the%20practice.

True threats, self-defense, and the Second Amendment. (n.d.). https://law.yale.edu/sites/default/files/area/center/justice/true_threats.pdf