Keith DeSantis
CS3043 Social Implications
Paper 4: Computer Security

Under the ethical framework of Kantianism, the United States, and any other country for that matter, should push for legislation promoting an international ban on cyber-attacks. At the moment, "the customary international law of countermeasures governs how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense—including, implicitly, cyber-attacks [1]." This precedent must be changed, and cyber-attacks must be discouraged through legislation if countries desire to remain in good standing ethically.

The alternative to banning cyber-attacks would be a "cyber-arms-race" of sorts between nations, as they strive to maintain their own security by creating better defenses and, most likely, stronger methods of attacking and breaking other nation's securities. To an extent this practice would be breaking the second formulation of Kantianism's Categorical Imperative [2]. As seen in situations like the Cold War, international arms races are incredibly dangerous and could wreak havoc in both the cyber and physical space. The nation's leaders and administrations would effectively be using the people of the world's safety and security as a means to the end of becoming a cyber superpower. Therefore, the only ethical course of action is to work towards a peaceful international ban of cyber-attacks.

This argument, however, does not take into account the realistic context of the USA and cyber-attacks, nor does it address the negative ethical effects of such a ban. The USA is already considered an "empire of hacking" by some nations, with organizations like the NSA having facilitated large scale cyber-incursions and attacks in the past [3]. Even if countries decided to ignore America's shady history and enter into legislative discussions, "any international agreement [would] necessarily define cyber-attack," which in and of itself is an endeavor, as the legal definition of a cyber-attack is rather vague and hard to pin down [4] [5]. Another point against this argument is that under Kantianism the autonomy of rational beings takes very high precedent and shouldn't be tampered with. By instituting such a ban, regardless of how altruistic the intentions, the government is removing the autonomy of the masses.

The key distinction in Kantianism, however, is the idea of removing autonomy for the betterment of humanity. While it is true that the ban would take away the autonomy of everyone, malicious or not, it would be doing it for the increased security and happiness of humanity as a whole. In the same way that outlawing murder and theft remove some form of autonomy, a ban of cyber-attacks would intrude on rational being's will but reap massive benefits for society as a whole. Cases like these are some of the only ones where Kantianism claims the actual removal of autonomy is the ethical choice, and not enforcing such rules is a passively unethical decision.

[1] O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, and J. Spiegel, “The Law of Cyber-Attack,” *California Law Review*, vol. 100, no. 4, p. 857, August 2012. Available: JSTOR, https://www.jstor.org/. [Accessed Nov. 17, 2020].

[2] M. Quinn, *Ethics for the Information Age*, 7th ed. New York, NY: Pearson, 2016. [E-book] Available: Yuzu E-book.

[3] M. Borak, “China calls the US an ‘empire of hacking’ following NSA advisory accusing Chinese hackers of exploiting cybersecurity bugs,” *South China Morning Post*, October 22, 2020. [Online], Available: https://www.scmp.com/tech/policy/article/3106613/china-calls-us-empire-hacking-following-nsa-advisory-accusing-chinese. [Accessed Nov. 17, 2020].

[4] S. Moore, “Cyber Attacks and the Beginnings of an International Cyber Treaty,” *North Carolina Journal of International Law and Commercial Regulation*, vol. 39, no. 1, p. 241, Fall 2013. Available: HeinOnline, https://heinonline.org/HOL/LandingPage?handle=hein.journals/ncjint39&div=10&id=&page=. [Accessed Nov. 17, 2020].

[5] United States Department of Homeland Security, “Cybersecurity,” *Department of Homeland Security*. [Online]. Available: https://www.dhs.gov/topic/cybersecurity. [Accessed Nov. 17, 2020].