CS 59866 – Senior Design Ethics Component

Azwad Shameem - 3/11/2022

Reaction Paper - Week 7

The blog post on the Council on Foreign Relations by Guest blogger for Net politics explicates that the general understanding of hacking back is linked the opening volleys of which may escalate into a kinetic war. The blog post clarifies that the only argument with some basis is that hacking back is that legally the use of force is a power reserved only for governments, and not private individuals and companies. However, the blog post also claims that a on a deeper analysis hacking back may not be seen as problematic as the general consensus. The blog post goes in depth of how the cyberspace is a borderland of sorts because the cyberspace is an ephemeral and unique domain that is hard to distinguish because of it’s a nature as a purely informational world and ever so slightly physical worldly bounds. The borders of a cyber attack are hard to locate in the first place even if it has clear physical roots. Furthermore, the cyberspace like a frontier, where cyberattacks are counted as frontier incidents, in which the UN declares that a frontier incident can’t invoke self-defense and escalation. The blog post goes into a detail orientated argument about how hacking back might actually be ethical or even reasonable. In my opinion, no matter how much legal or ethical reasoning there is for hacking back it doesn’t really match the risks involved because hacking back doesn’t really accomplish anything. Take for instance, the blog post’s own statements that it is hard to locate cyberattacks even if it has physical roots. Therefore, it would be very difficult to hack back at the actual attacker because it is hard to locate cyberattacks in general, so hacking back may lead to the innocents being attacked and in response those innocents might even attack back. In addition, I completely disagree with the blog post’s claim until authorities reliably defend our systems, hacking back may become the new normal because most of the individuals or companies that actually hack back do it to revindicate their reputation after being hacked. This is the case because if they did get hacked, in most cases they only have a general idea of where the attack is from not the exact individual or group.

The article, Forget Law and Ethics – Is Hacking Back Even Effective by Patrick Lin on Forbes clarifies the issue on hacking back. Lin states that in cybersecurity there is a sense of helplessness because in quite often in cybersecurity that is created is often the first and last line of defense for your information. In the digital world there is no rescue because the online life moves at digital speeds which law enforcement can’t match, in fact even the FBI often advise people to just pay the ransom. Lin also states that in 2015 a data breach at the U.S. Office of Personnel Management had more than 20 million federal workers records stolen including sensitive background information for security clearances. Hacking back in these incidents as a deterrent would most likely not deter malicious or ideological attacks but instead give them more incentives to attack even more. In my opinion, this is mostly correct because if you do hack back your attacker, whose to say they won’t attack again since they clearly have the confidence to do so. In fact, even if you did secretly hack back your information it may have already been too late, and the information could’ve been sold or shared to who knows how many. I believe that the only real reason to hack back is for self-satisfaction and restoration of your reputation as a individual or group because hacking back to protect yourself does little to nothing to deter your attacker and most likely will make another attack more likely.