Zelalem Yitbarek
CS-285L P-03 Professor A. Potasznik

Weekly Write-Up #4

When individuals or groups feel that their rights or interest are impaired by the state or organizations, they begin to oppose and confront different ways and strategies to impose their socio-political goal. Their opposition, activities, or strategies could be aline with the law. For that, they may invoke the first amendment to host and organize a protest to make their voices heard. On the contrary, they might choose to fight underground to become influential in a way that preserves what they believe is relevant. In this case, they are most likely to engage in illegal activities. They might tend to manipulate and use Computer technology as some form of battleground and as an opposition strategy. That can be considered an illegal act since they have a high chance of violating the **Computer Fraud And Abuse Act (CFAA)**. This criminal act protects a computer system or network access without authorization. **Hacktivism** is when a disruptive activity of the computer system or network of the state or organization in order to impose their goal or motive.

A hacktivist is a person or group who engaged in Hacktivism, as they move forward to influence and impose their Socio-Political interest they significantly damage the organization or government that might massively go to crises. They use various techniques to attack their targets, such as a Denial of Service (DoS), or releasing sensitive information after they steal it from the internet. The incident that happened to Turkish citizens would be a good example " Hacktivist groups have even wiped internal data belonging to target organizations, like ReadHack's erasure of over $670 billion in electricity bills belonging to Turkish citizens."(Insikt Group). The hacktivist intrusion sends the message to the company and Turkis government that they are capable of damaging the economy.

Even though Hacktivism is an illegal act, hacktivists considered themselves as social justice, democracy, and human rights advocacy group. These claims sound fair since the terms and their goals are exceptionally sensible, and the note they leave after the attack is sometimes agreeable. They left a note after they had attacked ISIS's website that may support their claim. "ISIS, We will hunt you. Take down your sites, accounts, emails, and expose you"(Wikipedia). Anyone who understood the inhumanity and animalistic behavior of ISIS might take such an attack as appropriate. On top of that, they involve significant protests in different parts of the world by either throw the decanters or bring equality. They involved in the recent Sudan revolution. "CrowdStrike says three groups claimed credit for the Sudan disruptions: Ghost Squad Hackers, Sudan Cyber Army, as well as the Brazil-based Pryzraky collective."(Schwartz). They play a crucial role in overthrowing the Al- Bashir government. However, through the eyes of their target and law, they are considered as cyber terrorists and illegal since they are explicitly violating laws such as CFAA.

Due to this, Law enforcement desperately look to hunt and brought Hacktivists to justice. However, the nature of hacktivists, decentralization, and hiding in the web would make prosecutors jab pretty hard. Besides, dozens of countries may pretend to be hacktivists or cooperate with the hacktivist behind the curtain for the sake of their political goal. In this case, the attack becomes beyond law enforcement capacity and may demand National security intervention to defend and backfire. That could open a door for cyberwar, which might be way more catastrophic than traditional war and impacts civilian life in all aspects.

In my opinion, hacktivism can be a double-edged sword that promotes computer intrusion, data theft, and violence for the sake of public good. Moreover, it has created a bunker for countries to attack each other. In both cases, civilians hold the burden on their shoulders and suffer substantially. Strong International law would be an excellent solution to address the problem. Enhancing technology in a way to overcome the attack and work towards highly skilled cybercops would help to mitigate the damage. Of course, there is no guarantee that the cybercops would not turn to hacktivists. That raises the question, **“Quis Custodiet Ipsos Custodes?”** which is “Who Watches the Watchers.”

Works Cited

Insikt Group “Return to Normalcy: False Flags and the Decline of International Hacktivism.” Record Future, Record Future, 21 August 2019
https://www.recordedfuture.com/international-hacktivism-analysis/

Wikipedia contributors. "Timeline of events associated with Anonymous." *Wikipedia, The Free Encyclopedia*. Wikipedia, The Free Encyclopedia, 9 Oct. 2019. Web. 26 Oct. 2019.

J.Schwartz, Mathew “Down and out in Hacktivist Land” Bank info Security, Bank Information Security Media Group, 23 August 2019
https://www.bankinfosecurity.com/down-out-in-hacktivist-land-a-12950