Topic 5 Discussion 2

Research the term "cyberwar." How does using the internet to wage a cyberwar affect personal and corporate privacy? Should only governments have the right to conduct cyber warfare? Where does the responsibility of corporations fit in the cyberwar landscape?

Hello Class,

In trying to figure out who should have access to cyberwar and how it affects companies we need to first know what cyberwar is and understand it. Cyberwar is or also known as cyberwarfare is exactly what it sounds like. It was a war or conflict that occurs in cyberspace. What happens is on computers virtual worlds are created and they attack each other. In this incident though instead of using guns and bombs they are using coding to attack the other computers, networks, and infrastructures. In these types of war, the objective or way to win is to disable, disrupt, or destroy the other persons computers, networks, and infrastructures. Items like malware, DDoS, and hacking are just a few of the weapons that are used in this circumstance (Kamen, 2023).

It's true that in the digital world, privacy is a constant challenge. Even the smallest traces of your online activity can be tracked, and this is often necessary for basic web functionality. However, it's important to be aware of the data you're sharing and to take steps to minimize your digital footprint. For businesses, the consequences of cyberattacks can be severe. Disruptions to operations can lead to lost wages, increased expenses, and reputational damage. Additionally, businesses can suffer from stolen data, loss of network access, and damage to their virtual systems. With individuals most the time it affects them with loss of personal and sensitive information, possible financial damages, and loss of their system (Kreisa, 2022).

While cyberwarfare often conjures images of nation-states and militaries engaged in conflict, the ethical implications of these attacks are rarely discussed. Just as we uphold ethical standards in traditional warfare, such as protecting medical facilities and providing care to prisoners, we should strive for similar ethical conduct in the cyber realm. If all cyberwarfare were conducted ethically, whether in real-world scenarios or training exercises, it could be argued that only governments should be allowed to engage in such activities. However, the reality is that many hackers operate outside of ethical boundaries, targeting individuals and organizations without regard for the consequences. This makes it imperative to establish clear guidelines and regulations for cyberwarfare, ensuring that it is conducted responsibly and with due consideration for the potential impact on civilians and critical infrastructure. If the attacker’s goal is to shut down a corrupt system than I could see it being ethical but not if their goal is to steal sensitive information to exploit it for money this is not ethical at all (Rowe, 2007). So, with ethics alone I do not feel government should be the only ones because if someone were to attack the business that I own with cyberwar than I feel I should be allowed to attack back with cyberwar to protect my assets.

In the modern era, corporations are increasingly intertwined with the realities of warfare, even in the cyber domain. As technology becomes ever more central to business operations, corporations bear a significant responsibility to safeguard the personal and sensitive information they hold. This responsibility is paramount given the inevitability of cyberattacks. It's no longer a question of if a corporation will be targeted, but when. The corporations responsibility for this is the safety and security of all technological items they control and everything within it (Zerlang, 2022). An example of a bank with them holding our money, account information, and personal information they are responsible to ensure that their security and safety is able to protect all of this information so that a hacker is not able to get access to our account and steal everything.

References:

Kamen, D. (2023, March 30). What is a Cyber War. NEIT. https://www.neit.edu/blog/what-is-acyber-war-explained

Kreisa, M. (2022, May 5). What is Cyberwarfare & How Does it hurts businesses?. PDQ. https://www.pdq.com/blog/impacts-of-cyberwarfare-on-businesses/

Rowe, N. C. (2007). Ethics of Cyberwar Attacks. Ethics of Cyberwar attacks. https://faculty.nps.edu/ncrowe/attackethics.htm

Zerlang, J. (2022, May 6). Cybersecurity is a corporate social responsibility, especially in times of war | venturebeat. Cybersecurity is a corporate social responsibility, especially in times of war. https://venturebeat.com/datadecisionmakers/cybersecurity-is-a-corporate-socialresponsibility-especially-in-times-of-war/