Lucas Esquivel

CS 462

Module 12: Assignment

Over the years technology has been growing at an astounding rate. Nowadays technology has become a necessary pillar to any countries military attack and defense operations. Nation states must make sure they have the best technologies with the best technological minds operating them if they want to get ahead of everybody else in the case there is a cyber war soon. Even though hacking into enemy systems and stealing potentially important congressional documents from another country is very different than being in a battlefield firing guns there are a few similarities between cyberspace and traditional wars. For example, cyberspace can be utilized as a weapon, just as tanks, guns and bombs can in a traditional war, cyberspace can be used to launch attacks like buffer overflows, SQL injections, and spyware. A country could use cyber to attack computer systems that control things like enemy drones and missiles. An example of that was the U.S making a cyber attack on Iran after Iran took down a U.S drone (*Secure World,* December 27, 2019).

High-tech, military grade, cyber military is still in its infant stages and there are many unknowns to just how powerful it can be. Wars used to be fought over land and between geographical lands with clear objectives. When you are in the cyber space it is very difficult to find exactly what you’re looking for. You could hack into a server expecting to find documents on things like manuals on how the enemies build their weapons but instead you end up in a server that’s just a database full of names of random civilians. That leads onto the next point I’m trying to make in that if not careful, cyberwarfare could impact the privacy of many innocent civilians potentially putting many people’s safety at risk. These cyber weapons are stealth ordinance, written in zeros and ones like all computer code. They have capabilities to shut down entire networks, infiltrate vulnerabilities and confuse enemy signals (Sue Halpern, July 18, 2019). Also, if there were a major cyber attack on the US that could destroy critical infrastructure it would be very difficult to detect things like point of attack, who the attacker is, and where the vulnerability is they exploited. With the added pressure of citizen’s lives at risk as well as damages to systems, it will be a major obstacle to overcome such attacks that were never seen anywhere else. Russia has recently been using cyber warfare against Ukraine to gather information targeting the Ukrainian government and financial banks. Things like protecting and preventing cyber attacks is very important for every section but I believe is even more important when we talk about the military because if there is a breach in the military it would lead to a huge safety concern for everybody.

It’s important that we adapt to the constantly evolving world of cyber space. Making sure the military is highly trained and has the most updated and high-tech resources around in order to defend and attack when necessary. Cyber war is where the battlefield is heading and it will definitely change the way nations go about using their military strategies.

Works Cited

Halpern, Sue. “How Cyber Weapons Are Changing the Landscape of Modern Warfare.” *The New Yorker*, 18 July 2019, https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare.

Team, SecureWorld News. “Cyber War vs. Traditional War: The Difference Is Fading.” *Cybersecurity Conferences & News*, Seguro Group, 16 Sept. 2020, https://www.secureworld.io/industry-news/cyber-war-vs-traditional-war.