CTC #6

2d Lt Marvin Newlin

CSCE 525

Lt Col Reith

24 Oct 18

Cyber weapons are a hot commodity on the market for countries and actors in cyberspace today. However, not much consensus exists on what exactly a cyber weapon is. The Tallinn manual on International Law Applicable to Cyber Conflict defines a cyber weapon as “cyber means of warfare that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack.1” This definition raises two of the most important characteristic of a cyber weapon in today’s world. That is the ability to inflict damage on a target, and somewhat more subtly, the ability to incapacitate a target.

Probably the most forefront example on a person’s mind when they think of a cyber attack is Stuxnet. Stuxnet was really the first time that the world saw the use of a cyber weapon to intentionally inflict damage on a system, both physically and logically. The Stuxnet worm infected systems particularly in Iran and altered the instruction of Industrial Control System (ICS) software which was the logical damage part. The physical damage part came because the physical systems whose instructions were being altered were nuclear centrifuges. These systems were extremely sensitive to altered instructions and the alterations caused the systems to malfunction. This example clearly demonstrates the damage characteristic of a cyber weapon.

Another characteristic of a cyber weapon is the ability to incapacitate. Physically can be viewed as an abstraction of the first, but in cyberspace where often systems are not damaged physically or logically, it is a separate category. One example of this characteristic is a denial of service attack.2 Even though a DoS attack doesn’t inflict physical/logical damage, it still possesses the same characteristics as a weapon because it prevents the target from operating. Consider the Russia/Georgia war of 2008. The Russians conducted DoS attacks on Georgian government websites which prevented them from communicating to the Georgian people and military. This DoS attack, although not physically damaging, had the same effect as dropping a bomb on the systems in that it silenced the systems that were targeted.

Notes

Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press, 2013.

Schmidle, R. E., Michael Sulmeyer, and B. Buchanan. "Non-Lethal Weapons and Cyber Capabilities." *Perkovich, G. and Levite, A., Understanding Cyber Conflict* 14 (2017).