Name: Ronit Singh **CDAD-UH 1037** **Date:** 26 September, 2021

CYBERWARFARE

Week 5 Reading Summary

The three assigned readings all focus on the topic of critical infrastructures and their protection. While the second reading is a research study that gives a more detailed account of a sophisticated and unusual cyber attack on a critical infrastructure in Iran and its implications. The third reading considers five key ethical questions in today's cyber realm (considering Stuxnet as an example) and answers or explains them in detail.

The first reading "Cybersecurity and Critical Infrastructure Protection" by James A. Lewis mentions that cyber security has been gaining attention lately and growing in importance with regards to critical infrastructure protection. According to the article, "An infrastructure is judged to be critical because it meets some standard of importance for the national interest—in that the goods or services it provides are essential to national security, economic vitality and way of life." (Lewis, 2006). The article points out that cyber security risks in critical infrastructures have been overanalyzed and overstated. It states that "critical infrastructures are dependent on computer networks for their operations. The chief flaw in this reasoning is that while computer networks are vulnerable to attack, the critical infrastructures they support are not equally vulnerable." (Lewis, 2006). "While the dependence on computer networks continues to grow, many critical functions remain insulated from cyber attack or capable of continuing to operate even when computer networks are degraded." (Lewis, 2006). This, apparently, is due to the redundancy of the internet and its ability to continue working even after an attack. Moreover, the article mentions the "human factor" that plays a key part in continuing the operations or functions after an attack. This does not pose a substantial risk to the security of the country and limits the attack. While in the context of terrorsim, "The complexity of successfully carrying out a cyber attack against national infrastructures like telecommunications or the electrical grid, combined with a lower probability of success than a physical attack, may make it unattractive to terrorists." (Lewis, 2006). Incidents like this seem to show that risk to critical infrastructures come primarily from physical attack.

The second reading "Stuxnet and the Future of Cyber War" by James P. Farwell & Rafal Rohozinski, presents research behind one of the world's first sophisticated and big-scale cyber attacks on a national level. It was a worm targeted to disrupt Iran's nuclear programme. The article, taking Stuxnet as an example, mentions the advantages of a cyber attack over physical means. Cyber attack is less costly than military action and poses an extremely less to no life risk at all to civilians as compared to traditional military means. In fact, it states that "the Stuxnet program cost was almost certainly less than the cost of a single fighter-bomber." (Farwell and Rohozinski). Stuxnet raises various questions regarding the ethics and forces the countries to advance their own cyber security programmes.

The third reading, "Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare" by Caroline Baylon discusses the key questions in ethics in the cyber realm with main concern on the nuclear sector. It mentions that even though Stuxnet would have attained its objectives, it would have only "postponed Iran's ability to develop nuclear weapons by 2 years, which is not a sizable achievement." (Baylon). Moreover,

by reverse engineering and taking inspiration from the attack, cybercriminals, terrorists, and criminal organizations have, without a doubt, enhanced their attacking capabilities and methodologies. The scale of the attack has created awareness and alerted several countries to improve their cyber capabilities. More and more countries are finding a way to get into the other nation's systems. Cyber espionage and planting of logic bombs (in case of conflict) are on the rise. Thus, Stuxnet seemed to do more harm than good, other than creating awareness.
However, nuclear facilities are still reluctant to give importance to cyber security due to cost cutting.

Moreover, the open source tools out on the internet for the "good" can be used by hackers for malicious purposes as well. Hence, restrictions on use and making vulnerabilities public can help maintain ethics in cyberspace. With increasing cyber attacks, there is a concern for ethics and it's an extremely important topic to be considered in the future.

What surprised me?

I was surprised to know the concept of hacking-for-hire companies that work for governments and private organizations or customers. They operate in the grey area and don't really care about ethics. They are money and profit-centric and don't usually disclose zero-day vulnerabilities to the public to prevent patches. I was also surprised to know that even the government intelligence agencies keep zero-day vulnerabilities secret to prevent patches and maintain their backdoor access for espionage or information gathering purposes. This approach seems to make the internet less secure, even for the public.

Moreover, planting of cyber weapons by nations, especially logic bombs, during peacetime to attack in case of a conflict seems surprising and marks a starting point for cyber warfare.

Questions?

1. What could be the various ways that the rise of cyber warfare between nations could be stopped?
2. What are the several stages of cyber warfare? Has it already begun taking place gradually on small scales? Will the general population get affected by it?
3. How can companies prevent bug bounty hunters from selling their zero-day vulnerabilities to other malicious organizations for money, especially considering the limitations of ethics and code of conduct in today's cyberspace?

References

A. Lewis, James. (2006). Cybersecurity and Critical Infrastructure Protection. Center for Strategic and International Studies, January 2006.

Baylon, Caroline. (2017). Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare. 10.1007/978-3-319-45300-2_12.

James P. Farwell & Rafal Rohozinski (2011) Stuxnet and the Future of Cyber War, Survival, 53:1, 23-40, DOI: 10.1080/00396338.2011.555586