Name: Ronit Singh **CDAD-UH 1037** **Date:** 7 November, 2021

CYBERWARFARE

Week 10 Reading Summary

All the assigned articles relate to attacks that have had a huge impact on a national level. The first article, *"Who is Anna-Senpai, the Mirai Worm Author?"* by Krebs on Security, dives deep into the **investigation of the actual mastermind** behind the Mirai botnet attack. The author explains the various steps he took and how he connected the dots to eventually lead him to its creator — **Paras Jha**. His friends considered him a good programmer, but an attention-seeker. The author says that his first breakthrough came when he linked the account name **'Anna-Senpai'** on **hackforums.net** (that released the Mirai source code to the public) to Paras Jha's LinkedIn profile based on a similar set of skills. There on, the author went down the rabbit hole to gather more information and evidence about him via chat messages, his comments on different forums, his resume etc. The article also mentions that he was a big fan of anime which inspired him to name his botnet 'Mirai' based on his favorite show **'Mirai Nikki'**.

The second article, *"A Guide to Cyber Attribution"* is about the ways law enforcement agencies use to come to conclusions and identify the criminals behind major cyber attacks. According to the article, **"cyber attribution"** is "the identification of the actor responsible for a cyber attack". The article says that the attackers (especially, nation state actors) "use cyber operations as a low-cost tool to advance their interests". Therefore, it's important to identify the ones responsible for these attacks and punish them. It mentions three key indicators of attribution namely, **tradecraft, infrastructure, malware, and intent**. It also outlines various best practices for determining attribution such as analysing and identifying through **errors** made by the creator unknowingly, **timely collaboration, information sharing, and documentation** among private security firms, agencies, victims, analysts, and politicians, and applying **rigorous analytic tradecraft knowledge** to observe and uncover data. In the end, the article includes a representation showing some of the famous cyber attacks and what factors or indicators led to the conclusion of attributing it to a specific country.

The third article is a newspaper report on a cyber incident that led Microsoft to accuse Russia behind a cyber attack based on the ways of attribution. It mentioned that the hackers were supported by or linked to the Kremlin (the Russian government). However, there was not enough evidence to make such a claim and the Russian government openly denied their involvement. Moreover, the claims suggest that it was done with the aim to interfere with US elections at that time. However, due to the lack of evidence, thus explaining the reason behind the title 'faith-based attribution', the whole claim was dismissed.

The fourth article, *"Grey Zones in the International Law of Cyberspace"* raises issues regarding laws concerning cybersecurity and calls the gaps in these laws **'grey zones'** where nothing is concrete. According to the article, grey zones are the "areas of law where the application of traditional principles and rules is unsettled". Moreover, the article outlines the following grey zones present today namely, **"sovereignty, intervention, the use of force, self-defense, and international humanitarian law"**. It is important that these grey areas be rectified so as to prevent the exploitation of these by malicious actors due to the ambiguities.

What surprised me?

I was surprised to know that the man behind the Mirai botnet attack was himself a founder of a security company - ProTraf, that helped other companies in mitigating DDoS attacks. Moreover, the whole sequence of events, chat / forum messages, and interviews and how the author went on to unpuzzle each piece and connect with the other amazed me.

Questions?

1. What motivates hackers to do DDoS attacks? Was the main motive of the Mirai botnet attack financial gain or to seek attention by intentionally exploiting easily vulnerable IoT devices?
2. How can hacking incidents result in election meddling? Does it have a direct or an indirect impact?

Works Cited

Krebs on Security, Who is Anna-Senpai, the Mirai Worm Author? (January 18, 2017). https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

RT. "'Faith-Based Attribution': Microsoft Unable to Identify Those Behind Pre-Midterm Hacking – Experts." RT International, 15 May 2020, www.rt.com/usa/436519-microsoft-russian-hacking-assumption

Schmitt, Michael N., Grey Zones in the International Law of Cyberspace (October 18, 2017). 42:2 Yale Journal of International Law Online 1 (2017), Available at SSRN: https://ssrn.com/abstract=3180687

A Guide to Cyber Attribution - Dni.gov. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf