Collaborative Discussion 1 – Peer Response 3 – Kingsley Omyeemeosi

Thank you Kingsley for your extremely interesting post, which inspired me to reflect critically on ethical cyber security.

In July 2016, the North Atlantic Tready Organization (NATO) published a Cyber Defense Pledge, which addresses the security threats posed by cyber attacks and is intended to improve the cyber defense of the national infrastructure (Christen et al., 2020: 206).

A cyber attack on the Iranian power grid that took place in 2010 shows that this goal is of great importance. In June 2010, a malicious computer worm named Stuxnet was discovered that was specially developed to monitor and control a Siemens system. The system controls frequency converters that have the task of regulating the speed of motors (Fallier et al., 2010: 32-42). Such frequency converters are used for industrial plants such as waterworks, but also uranium enrichment plants and nuclear power plants. In September 2010, Iran confirmed Stuxnet's cyberattacks. 30,000 computers are said to have been affected without causing serious damage, but the power grid was affected (Heise, 2010).

How credible this statement is, however, is doubtful, since both parties allegedly involved, the USA and Iran, subsequently denied the development or the damage (Spiegel, 2010). It was only found in 2012 that, contrary to the statement, the USA and Israel had commissioned the development of the software (Nakashima & Warrick, 2012). The following years show that this software was not only used for its (probably) original purpose. In 2012, it is believed that the developers of the malware lost control of the program (Anderson 2012). In 2014 the malware was found in a German nuclear power plant. Espionage is presumed to be the intension (University of Hawai'I, N.D.).

However, what a malicious, destructive intervention in nuclear power plants could mean can be seen in the two accidents in Chernobyl and Fukushima, in which errors in the control system (in both cases due to a technical failure) led to a nuclear catastrophe. It is therefore not wrong to claim that: "Cyberspace is now seen as the fifth military battlefield alongside ground, air, water and space" (Heise, 2010).

On the basis of this history, every cyber security specialist, but also programmer in general, should be clear about the scope of their actions in order to be able to make ethically correct decisions.

References:

Anderson, N. (2012) Confirmed: US and Israel created Stuxnet, lost control of it. ARS Technica. Available from: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ [Accessed:18.08.2021]

Christen, M., Gorijn, B., Loi, M. (2020) The Ethics of Cybersecurity. Springer. Available from: https://library.oapen.org/bitstream/handle/20.500.12657/22489/1007696.pdf?sequence=1&isAllowed=y [Accessed: 18.08.2021]

Fallier, N., Murchu, L., Chien, E. (2010) W32. Stuxnet Dossier. Symantec. Available from: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf [Accessed: 18.08.2021]

Heise (2010) Iran bestätigt Cyber-Angriff durch Stuxnet. Available from: https://www.heise.de/security/meldung/Iran-bestaetigt-Cyber-Angriff-durch-Stuxnet-Update-1096365.html [Accessed: 18.08.2021]

Nakashima, E. & Warrick, J. (2012) Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. Avialable from: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [Accessed: 18.08.2021]

Spiegel (2010) Iran wirft Westen Cyber-Propaganda vor. Available from: https://www.spiegel.de/netzwelt/netzpolitik/stuxnet-angriff-iran-wirft-westen-cyber-propaganda-vor-a-720043.html [Accessed: 18.08.2021]

University of Hawai'I – West O'ahu (N.D.) Cyber Attack on German Nuclear Power Plant. Available from: https://westoahu.hawaii.edu/cyber/regional/world-news-europe/cyber-attack-on-german-nuclear-power-plant/ [Accessed: 18.08.2021]