Collaborative Discussion 1: Summary Post

Rogue Services was a web hosting service whose unique selling proposition was “cheap, guaranteed uptime, no matter what” (ACM, 2018). As a result, a majority of Rogue’s customers hosted malware, managed botnets, and spammed online victims (ACM, 2018). Multiple internet service providers, government organisations, and security firms requested that Rogue remove these bad actors from their service; however, Rogue refused all such requests, citing that their user agreements and host nation laws absolved them from taking any clients offline (ACM, 2018). As a result, security vendors coordinated with several government authorities to take Rogue offline by force with a worm and denial-of-service attack which immediately reduced predatory internet activity (ACM, 2018).

Rogue was clearly violating tenets of the BCS Code of Conduct, blatantly disregarding the “health, privacy, security and wellbeing of others” (BCS, 2022) and by taking “action which could bring the profession into disrepute” (BCS, 2022). The security firms responsible for taking down Rogue adhered to the BCS Code since they acted in the public interest, and in accordance with the authorities they serve (BCS, 2022). However, the United Nations Office on Drugs and Crime indicates that communications infrastructure is part of a nation’s territorial sovereignty and that access to this infrastructure without host nation approval is still a violation of that nation’s sovereignty – even if investigating crime (UNODC, 2019). Additional considerations concerning jurisdiction for investigation and action include the nationality of the cyber criminals and victims involved, but without specific accords guaranteed by affected nations, this topic is still highly contentious (UNODC, 2019).

In a world where the boundaries between virtual and physical worlds continue to blur, the notion of cyber attacks constituting an “act of war” has become a focal point for governments across the globe (Libicki, 2009, Vindman, 2021). Despite the good intentions posed by the security vendors and governments, taking such offensive action without host nation permission could be seen as an act of aggression and prompt a retaliatory attack in the name of self-defence (Schmitt, 2020; Vindman, 2021).

Response posts from classmates affirmed the position of this discussion, and feedback from my tutor provided useful suggestions to improve future posts.

References

ACM. (2018). *Case: Malware Disruption*. [online] Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/. [Accessed 11 Nov. 2022].

BCS (2022). *BCS Code of Conduct*. [online] BCS. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/. [Accessed 11 Nov. 2022].

Libicki, M.C. (2009). *Cyberdeterrence and Cyberwar*. [online] www.rand.org. Available from: https://www.rand.org/pubs/monographs/MG877.html. [Accessed 11 Nov. 2022].

Schmitt, M. (2020). *Russia's SolarWinds Operation and International Law*. [online] Just Security. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/. [Accessed 11 Nov. 2022].

UNODC (2019). *Cybercrime Module 7 Key Issues: Sovereignty and Jurisdiction*. [online] United Nations Office on Drugs and Crime. Available from: https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html. [Accessed 11 Nov. 2022].

Vindman, Y. (2021). *Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is.* [online] Lawfare. Available from: https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it. [Accessed 11 Nov. 2022].