Discussion – Summary post:

In my initial post, I thoroughly examined the captivating ‘Case: Malware Disruption, Using the Code: Malware Disruption’ (ACM Ethics, 2018), a pivotal study that illuminates the intricate interplay between the legal, social, and professional dimensions of cybersecurity. I also emphasised the violations of the BCS Code of Conduct (BCS, 2022) compared with the ACM Code of Ethics and Professional Conduct (ACM, 2018), which are fundamental for understanding ethical practices in our field.

My colleagues Steve and Maria have responded to my post with valuable and thoughtful insights. Steve highlighted my referencing mistakes and contributed to my initial post, sharing the Budapest Convention (ETS No. 185) and Protocols. The Budapest Convention by the Council of Europe (2014), also known as the Convention on Cybercrime, aims to combat cybercrime through international cooperation and seeks to harmonise national laws, improve investigation and prosecution through electronic evidence collection, and establish channels for collaboration between member states on police and judicial matters. Optional protocols address specific areas like hate speech online, enhancing international cooperation and combating cybercrime effectively. This was an excellent addition to reflect on my initial post since I highlighted international collaboration in cybercrimes.

On the other hand, my colleague Maria sparked my thoughts by mentioning ethical hacking and contributing significantly to my research on white and red hats. I have found that in the cyber-war, it is crucial to distinguish between white-hat and black-hat hackers. White-hat hackers aim to combat and raise awareness through education and

training, while black-hat hackers use malicious intent to cause harm. Grey-hat hackers can switch between black-hat and white-hat hacking (Yaacoub et al. 2021).

My chosen case is debatable since cybersecurity intentions are ambiguous, as highlighted by Lahcen et al. (2020). This case prompts discussions on ethically sound alternatives to tackling Rogue Services and establishes clear guidelines for acceptable cybercrime responses within the industry.

References:

ACM (2018). *ACM Code of Ethics and Professional Conduct*. [online] Association for Computing Machinery. Available from: https://www.acm.org/code-of-ethics [Accessed 18 May 2024].

ACM Ethics. (2018). *Case: Malware Disruption*. [online] Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 17 May 2024].

BCS (2022). *BCS, THE CHARTERED INSTITUTE FOR IT CODE OF CONDUCT FOR BCS MEMBERS*. [online] Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 18 May 2024].

Council of Europe (2014). *Budapest Convention and related standards*. [online] Cybercrime. Available from: https://www.coe.int/en/web/cybercrime/the-budapest-convention [Accessed 18 May 2024].

Lahcen, R.A.M., Caulkins, B., Mohapatra, R. & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, [online] 3(1). doi:https://doi.org/10.1186/s42400-020-00050-w.

Yaacoub, J.A., Noura, H., Salman, O. & Chehab, A. (2021). *A Survey on Ethical Hacking: Issues and Challenges*. [online] ResearchGate. Available from: https://www.researchgate.net/publication/350483773_A_Survey_on_Ethical_Hacking_Issues_and_Challenges [Accessed 17 May 2024].