Discussion: Peer Response 1:

Hi Maria,

Your topic is fascinating as it concerns the behaviour of individuals in a work environment. Your analysis of the ACM case study by ACM Ethics (2018) on abusive workplace behaviour was insightful. By comparing it to the relevant codes of the ACM (2018) and BCS (2022), you have highlighted some critical differences, emphasising ethics, psychological safety, and legal compliance. I agree that psychological safety is essential for fostering a healthy work environment, and accountability plays a crucial role in addressing abusive behaviour. We need a solution-oriented approach to enforcing ethical policies, as stated by the European Commission (2021).

The global study conducted by Ferrère et al. (2022) is a testament to the universal importance of psychological safety in the workplace. This shared belief encourages employees to take interpersonal risks and is crucial for an organisation's ethical climate. Leaders and compliance officers can leverage this understanding to promote timely changes, encourage misconduct reporting, and ensure team effectiveness, well-being, and moral culture, regardless of geographical location.

Your post highlights some thought-provoking areas for further exploration. The study by Weinbaum et al. (2019) underscores the complexity of ethics, shaped by historical events, ethical lapses, scientific advancements, and cultural values. Seth (N.D.) rightly points out the inadequacy of the ACM Code of Ethics in defining ethical goals for computing systems, leading to unjust outcomes. To address this, ethical principles should encompass both terminal and instrumental values (Openstax, N.D.).

Peer Response 2:

Hi Steve,

I wanted to express my gratitude for responding to my initial post. Thank you for your comments and for pointing out my errors regarding the reference. I will be more careful in the future, especially since we are submitting our final projects.

When I highlighted the Crown Prosecution Service (2019) notes, I wanted to show the relationship between economic-related cybercrimes involving unauthorised access, sabotage, or use of computer systems for financial gain or loss. According to the Crown Prosecution Service (2019), intellectual property crime involves unauthorised use of copyrighted material, including counterfeiting, piracy, and technology development for profit, while piracy involves profit-driven copying of original recordings.

Regarding the legal grey area, I wanted to emphasise the concept of international cooperation in cybersecurity. This concept is of utmost importance, as highlighted by Michael Warner's Intelligence in Cyber—and Cyber in Intelligence (Levite & Perkovich, 2017), article, page 19. The article states, and I quote, "though certainly a fair amount of illegal or at least unethical mischief is directed against the software sold to consumers to facilitate the harvesting and sale of their data. Going from such mischief to actively cyber-spying on unsuspecting people is a short step. Today, anyone with a network connection can be a victim of espionage mounted from nearly anywhere."

Your reminder about the chatbot study skills article on referencing was spot on. I will take the time to study it thoroughly. Thank you for sharing the Budapest Convention (ETS No. 185) and its Protocols.

Regards, Hainadine

Peer Response 3:

Hi Maria,

I appreciate your thoughtful response to my post. The post discusses a Red Hat hacking strategy involving a self-replicating worm to disrupt Rogue Services, a company facilitating malicious activities. According to Yaacoub et al. (2021), Red Hat hackers use extreme tactics to combat black hat, malicious hackers, relying on offence over defence. They destroy devices through viruses or data retrieval. The worm's creators targeted Rogue Services' entire network (ACM Ethics, 2018), potentially causing collateral damage to innocent clients. The legality of the worm's deployment is debatable, as it involved unauthorised access and data destruction, making it an aggressive and potentially risky tactic (Broeders, 2021).

The ethical spectrum in cybersecurity is complex, with a self-replicating worm potentially aligning with white hat goals and causing unintended consequences. The worm's creators may fall somewhere between a "grey hat" action with a debatable ethical stance. As Morgan et al. (2021) note, "white hats are ethical hackers who have been given the authority by the system's owner to test for security vulnerabilities." Regarding the table, here is a revised table with additional columns:

Action/Actor	Legal	Social	Professional	ACM Principle
Rogue Services' operation	Breach	Detrimental	Breaches BCS 1 & 2 (BCS, 2022).	1.1, 1.2, 2.8 (ACM, 2018).
Creation of denial-of-service worm	Grey Area	Potentially beneficial	Debatable (depends on perspective)	1.2, 2.8 (arguably)

This case underscores the ambiguity of cybersecurity intentions, prompting discussions on ethically sound alternatives to tackling Rogue Services and establishing clear guidelines for acceptable cybercrime responses within the industry, as highlighted by Lahcen et al. (2020).

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 7 May 2024].

ACM Ethics. (2018). *Case: Abusive Workplace Behavior*. [online] Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-abusive-workplace-behavior/ [Accessed 7 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 7 May 2024].

Broeders, D. (2021). Private active cyber defense and (international) cyber security—pushing the line? *Journal of Cybersecurity*, 7(1). doi:https://doi.org/10.1093/cybsec/tyab010.

Crown Prosecution Service (2019). *Cybercrime - Prosecution Guidance*. [online] Cps.gov.uk. Available from: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance [Accessed 5th May 2021].

European Commission (2021). *Ethics By Design and Ethics of Use Approaches for Artificial Intelligence*. [online] Available from: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf [Accessed 7 May 2024].

Ferrère, A., Rider, C., Renerte, B. & Edmondson, A. (2022). Fostering Ethical Conduct Through Psychological Safety. *MIT Sloan Management Review*, [online] 63(4). Available from: https://sloanreview.mit.edu/article/fostering-ethical-conduct-through-psychological-safety/ [Accessed 7 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.

Levite, A. & Perkovich, G. (2017). *UNDERSTANDING CYBER CONFLICT 1 4 A N A L O G I E S EDITORS*. [online] Available from: https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_FullText.pdf [Accessed 5th May 2021].

Morgan, G., Gordijn, B., Lewis, D. & Moorkens, J. (2021). *Ethical Issues in Cybersecurity: Employing red teams, responding to ransomware attacks and attempting botnet takedowns*. [online] Available from: https://doras.dcu.ie/26226/1/PhD%20Gwenyth%20Morgan.pdf [Accessed 17 May 2024].

Openstax (N.D.). *5.2 Dimensions of Ethics: The Individual Level - Principles of Management | OpenStax*. [online] Available from:

https://openstax.org/books/principles-management/pages/5-2-dimensions-of-ethics-the-individual-level [Accessed 7 May 2024].

Seth, A. (N.D.). *What's Missing in the ACM Code of Ethics and Professional Conduct | ACM Interactions.* [online] Available from: https://interactions.acm.org/archive/view/may-june-2023/whats-missing-in-the-acm-code-of-ethics-and-professional-conduct [Accessed 7 May 2024].

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].

Weinbaum, C., Landree, E., Blumenthal, M., Piquado, T. & Ignacio Gutierrez (2019). *Ethics in Scientific Research An Examination of Ethical Principles and Emerging Topics.* [online] Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2912/RAND_RR2912.pdf [Accessed 7 May 2024].