ePortfolio Activity: Collaborative Learning Discussion 1

Initial post:

I have selected the case study 'Malware Disruption', highlighting the complex relationship between cybersecurity's legal, social, and professional aspects.

As Crown Prosecution Service (2019) notes, Rogue Services violated several laws and evaded the consequences of their actions, such as financial losses, identity theft, and data breaches. The negative social impact of Rogue Services' actions, including financial losses, identity theft, and data breaches, raises concerns about the permissibility of vigilantism in cybersecurity, as highlighted by Cremer et al. (2022).

The ethical dilemma surrounding using a denial-of-service worm is a topic of intense debate. Its successful use to halt malicious activity creates a legal grey area. Levite & Perkovich (2017) argue that this situation raises profound questions about the boundaries of vigilantism in cybersecurity, a weighty consideration in our field.

The breach of professional ethics by Rogue Services, driven by profit rather than public good, led to the violation of the BCS Code of Conduct (BCS, 2022) and ACM Code of Ethics and Professional Conduct (ACM, 2018).

I would recommend strengthening international cooperation on cybersecurity regulations and laws, such as cybercrime and data protection laws, as UNODC (2019) emphasises. Collaboration and clear frameworks are needed to address these issues effectively.

The violations of the ACM Code of Ethics and Professional Conduct in comparison to the BCS Code of Conduct are the following:

ACM Code of Ethics and Professional Conduct	BCS Code of Conduct
1.1. Contribute to society and human well-being, acknowledging that all people are stakeholders in computing	Clause 2: Professional Competence and Integrity
1.2. Avoid harm	Clause 4: Duty to the Profession
2.8. Access computing and communication resources only when authorised or compelled by the public good	Clause 1: Public Interest
3.1. Ensure that the public good is the central concern during all professional computing work	Clause 1: Public Interest

References:

- Crown Prosecution Service (2019). *Cybercrime - Prosecution Guidance*. [online] Cps.gov.uk. Available from: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, [online] 47(3). Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/.
- Levite, A. and 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.
- 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.
- ACM (2018). *ACM Code of Ethics and Professional Conduct*. [online] Association for Computing Machinery. Available from: https://www.acm.org/code-of-ethics.
- UNODC. (2019). *Cybercrime Module 8 Key Issues: International Cooperation on Cybersecurity Matters*. [online] www.unodc.org. Available from: https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html.