The malware disruption case study focuses on legal, social, and professionally concerns pertaining to the ACM Code of Ethics (ACM, 2018) and the British Computer Society (BCS) Code of Conduct (BCS, n.d.). Since Distributed Denial of Service (DDoS) cyberattacks impact companies in many countries, jurisdictional difficulties develop, requiring international law enforcement cooperation. While mitigating security concerns, both the ACM (1.2) and BCS (Public Interest) Codes stress minimising damage and considering the public interest.

Non-jurisdictional issues include unforeseen effects of mitigation attempts, such as blocking the Internet connectivity of innocent consumers (ACM, 2018, 1.2; BCS, n.d., Public Interest). The importance of good communication among stakeholders, such as law enforcement, internet service providers, and the general public, is highlighted by social concerns. Both Codes (ACM, 2018, 2.7; BCS, n.d., Public Interest) emphasise the need for enhancing the public's awareness of computing and ensuring fair access to IT advantages.

Professionalism is essential, since computer professionals must exhibit ethical behaviour, continuous professional growth, and adherence to cybersecurity best practises (ACM, 2018, Principle 6; BCS, n.d., Professional Competence and Integrity).

In conclusion, the case study highlights the significance of addressing legal, social, and professionalism concerns in cybersecurity. Professionals in computing must conform to ethical standards (ACM, 2018; BCS, n.d.), engage with international law enforcement, evaluate unintended effects, communicate effectively, and maintain professional competence.

References:

ACM. (2018). ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/code-of-ethics/ [Accessed: 27 March 2023].

BCS. (n.d.). BCS Code of Conduct. Available from: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed: 27 March 2023].