Hypothetical scenarios are useful for testing the application of ethical computing principles. The ACM (n.d.a) presented a fictional scenario where a web host (Rogue) provided strong uptime guarantees for all of its websites, "no matter what". Bad actors abused this guarantee by hosting malicious software on Rogue's infrastructure, which were harmful to the internet at large. These bad actors were the majority of Rogue's client base.

Despite requests from various groups to remove the bad actors, Rogue refused to do this because of their "no matter what" principle. Government intervention was also not possible due to relaxed hosting laws in Rogue's country of origin. Consequently, security vendors and government groups decided to use a targeted computer worm to destroy Rogue's infrastructure. Consequently, all of Rogue's clients were taken offline- this included some legitimate e-commerce websites.

The ACM briefly discussed the application of their principles to this scenario, though it can be argued that the application of their principles was imperfect here. The ACM stated that the use of a worm was consistent with principle 1.2 of its code (ACM, n.d.b) because there was a moral basis for its use- removing malicious software from the internet is in the best interest of the public. They conceded that more could have been done to protect Rogue's legitimate clients from harm, however, this is insufficient- principle 1.2 clearly states that those responsible for unintended harm "are obliged to undo or mitigate the harm as much as possible". As the legitimate clients were e-commerce stores and the teams responsible for writing the worm understood the scope of Rogue's systems well, it is reasonable to state that it was negligent (and unjust) of the developers to not collect the details of legitimate clients and warn them of the attack so their data could be saved. This arguably constitutes a violation of principle 1.2, even if that principle was adhered to elsewhere. The ACM's discussion does not mention the legal implications of this approach- principle 2.3 tells professionals to respect local and international laws, although in this case study, government organisations were involved with the worm's development, so it is likely that this solution was lawful in nature (at least within the countries where the developers are located).

From the perspective of the BCS Code of Conduct (BCS, 2022), the actions taken by the worm authors were mostly acceptable. Section 1a states that professionals should take the security wellbeing of others into consideration, and it can be said that destroying malicious operations achieves this outcome. Section 2f states that professionals should avoid harming others through malicious actions; in this case, the actions taken were harmful but not malicious in nature, thus it can be argued that the two sections are not in conflict with each other. However, the harm of legitimate website owners does violate this principle. Furthermore, section 4a states that professionals must not do anything that tarnishes the image of the field; the use of a worm in this situation would not do such a thing. Lastly, section 2d encourages compliance with laws and regulations, but as mentioned above, the involvement of government organisations implies that the actions taken here were lawful for the countries where the developers are located.

From the perspective of UK legislation, the actions taken here would be illegal. Section 3 of Computer Misuse Act 1990 (CMA), states that it is an offence to perform "an unauthorised act with the intent to impair the operation of a computer" (CPS, 2019). Critics argue that the act is currently too broad in scope, as it makes it difficult (and sometimes illegal) to use hacking techniques for legitimate and good purposes (Rapid7, 2021; Guinchard, 2017). In 2021, the UK Home Office requested consultation on how the law should be adjusted, and therein, a campaigning group (CyberUp) argued that the act should protect security professionals working in the public interest, furthermore, they argued that the authorisation necessary for such acts should be reduced (House of Commons Library, 2022). Such a change would completely protect the professionals in this scenario. On 19 April 2022, a debate was held on revising the act (UK Parliament, 2022). It remains to be seen how the act will be adjusted based on discussions.

One final consideration is the legislation of the country that Rogue operates in, and whether that impacts the legality of the work the worm developers have done, however, the country is not specified.

**References**

ACM. (n.d.a) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 18 June 2022].

ACM. (n.d.b) ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/ [Accessed 18 June 2022].

BCS. (2022) BCS Code of Conduct. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 18 June 2022].

CPS. (2019) Cybercrime - prosecution guidance. Available from: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance [Accessed 18 June 2022].

Guinchard, A. (2017) The Computer Misuse Act 1990 to Support Vulnerability Research? Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime. Journal of Information Rights, Policy and Practice 2(2): 1-35. DOI: http://dx.doi.org/10.2139/ssrn.2946763

House of Commons Library. (2022) Debate Pack- Westminster Hall debate on the Computer Misuse Act 1990. Available from: https://researchbriefings.files.parliament.uk/documents/CDP-2022-0082/CDP-2022-0082.pdf [Accessed 18 June 2022].

Rapid7. (2021) Reforming the UK’s Computer Misuse Act. Available from: https://www.rapid7.com/blog/post/2021/08/12/reforming-the-uks-computer-misuse-act/ [Accessed 18 June 2022].

UK Parliament. (2022) Computer Misuse Act 1990 Volume 712: debated on Tuesday 19 April 2022. Available from: https://hansard.parliament.uk/Commons/2022-04-19/debates/AE9413F3-D4F2-44EC-890E-75B0250328C4/ComputerMisuseAct1990 [Accessed 18 June 2022].