**Peer response 1 – Ketan**

Your analysis effectively captures the core ethical tensions in malware disruption, particularly highlighting how the ACM's "avoid harm" principle creates complex decision-making scenarios when protective actions risk unintended consequences (Association for Computing Machinery, 2018). The jurisdictional complications you identify are especially pertinent, as cyber operations inherently transcend traditional legal boundaries, creating scenarios where well-intentioned interventions may violate sovereignty or local regulations.

Your comparative analysis between ACM and BCS codes reveals important distinctions in professional emphasis. The ACM's Section 2.8 specifically addresses unauthorized access for public good, stating that "under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others." This provides more explicit guidance than the BCS code regarding malware disruption scenarios (British Computing Society, 2022). Literature demonstrates how these ethical balances can be struck: the 2017 WannaCry ransomware incident illustrates both successful and problematic approaches — while Marcus Hutchins' kill switch activation prevented widespread damage, subsequent legal complications highlighted jurisdictional complexities (Hern and Levin, 2017). Similarly, the Conficker Working Group's collaborative approach in 2008-2010 demonstrates how multi-stakeholder coordination can address ACM Section 2.5's requirement for "comprehensive and thorough evaluations" while respecting sovereignty concerns (Bowden, 2011). The NotPetya attribution and response efforts further exemplify how professional competence requirements (ACM Section 2.6, BCS Section 2.1) necessitate specialized cybersecurity expertise and international cooperation frameworks.

Your conclusion aptly synthesizes the multifaceted nature of professional computing ethics. These historical precedents reinforce both codes' underlying premise that computing professionals must balance technical capability with ethical reasoning, legal compliance, and social responsibility, particularly when actions affect critical infrastructure and cross jurisdictional boundaries.

**References:**

Association for Computing Machinery (2018) ‘Code of Ethics’. Available at: https://www.acm.org/code-of-ethics (Accessed: 31 August 2025).

Bowden, M. (2011) *Worm: The First Digital World War*. 1st edn. New York: Atlantic Monthly Press. Available at: https://www.softouch.on.ca/kb/data/Worm.%20The%20First%20Digital%20World%20War.pdf.

British Computing Society (2022) *BCS Code of Conduct for members - Ethics for IT professionals*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct (Accessed: 31 August 2025).

Hern, A. and Levin, S. (2017) ‘Briton who stopped WannaCry attack arrested over separate malware claims’, *The Guardian*, 3 August. Available at: https://www.theguardian.com/technology/2017/aug/03/researcher-who-stopped-wannacry-ransomware-detained-in-us (Accessed: 31 August 2025).