

## Question

### **Should cybersecurity incident responders follow deontological rules or utilitarian outcomes when deciding whether to "hack back" against active attackers?**

---

When a ransomware attack locks down a hospital's electronic health records system, threatening patient lives, should the cybersecurity incident response team be allowed to "hack back" into the attacker's command-and-control server to retrieve decryption keys and shut down the attack? This scenario, increasingly common in today's threat landscape where ransomware attacks increased 13% in 2022 affecting healthcare, finance, and critical infrastructure sectors (Verizon, 2023), raises fundamental questions about the ethical frameworks that should guide cybersecurity professionals' decision-making during active incidents.

The Cybersecurity and Infrastructure Security Agency's (CISA) Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (2024) establish that incident response must follow standardized coordination procedures through official channels, with "threat response" activities, including offensive operations to identify, pursue, and disrupt threat actors, explicitly designated to law enforcement and intelligence agencies (FBI, DOJ, NSA), not private sector incident responders. This framework of required coordination and role separation reflects a deontological approach: cybersecurity professionals have a duty to follow established protocols regardless of immediate consequences.

From a deontological perspective grounded in Kant's Categorical Imperative, unauthorized access to an attacker's systems, even in self-defense, violates the universal principle that we must not access computers without authorization. If every victim organization adopted "hack back" as standard practice, the resulting chaos, misattribution, and escalation would undermine the rule of law in cyberspace (Lin, 2016). Professional codes of ethics, including the ACM Code of Ethics and Professional Conduct, obligate IT professionals to "avoid harm" and "be honest and trustworthy," which includes not engaging in unauthorized system access even against malicious actors (Gotterbarn & Miller, 2009).

However, a utilitarian perspective might argue that hacking back produces the greatest good for the greatest number when it prevents catastrophic harm. In the hospital ransomware scenario, unauthorized retrieval of decryption keys could save lives, a consequence that outweighs abstract rule-following. The Active Cyber Defense Certainty Act (proposed but not enacted) attempted to codify this consequentialist reasoning by permitting limited defensive intrusions under specific conditions (U.S. Congress, 2019).

Moor's Just Consequentialism framework offers a potential middle path: incident responders should deliberate from an impartial perspective to identify policies that avoid unnecessary harm while supporting fundamental rights. This might justify hack-back only when coordinated with law enforcement, preventing both the harm of unchecked attacks and the harm of vigilante cyber operations.

Given the policy vacuum around active defense and the competing ethical frameworks at stake, which ethical approach, rule deontology, act utilitarianism, or Just Consequentialism, should guide cybersecurity incident response teams when facing active attacks? Should professional duty to follow coordination protocols override consequentialist calculations about preventing immediate harm?

## References

- Cybersecurity and Infrastructure Security Agency (CISA). (2024).** *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*. U.S. Department of Homeland Security.  
[https://www.cisa.gov/sites/default/files/2024-08/Federal\\_Government\\_Cybersecurity\\_Incident\\_and\\_Vulnerability\\_Response\\_Playbooks\\_508C.pdf](https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf)
- Verizon Enterprise. (2023). 2023 Data Breach Investigations Report. Verizon Communications.  
<https://www.verizon.com/business/resources/reports/dbir/>
- Lin, H. S. (2010). *Offensive cyber operations and the use of force* (Journal of National Security Law & Policy, Vol. 4:63). Georgetown University Law Center.  
[https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2010/08/06\\_Lin.pdf](https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2010/08/06_Lin.pdf)

**Gotterbarn, D., & Miller, K. W. (2009).** The Public is the Priority: Making Decisions Using the Software Engineering Code of Ethics. *IEEE Computer*, 42(6), 66-73.  
<https://doi.org/10.1109/MC.2009.204>

**Berris, P. G. (2020).** *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress* (CRS Report No. R46536). Congressional Research Service.  
<https://crsreports.congress.gov/product/pdf/R/R46536>