Issues in Information Systems
Volume 26, Issue 1, pp. 194-200, 2025

DOI: https://doi.org/10.48009/1_iis_2025_115

Hack back or step back? Exploring an ethical dilemma between cyber defense and cyber vigilantism

Donna Schaeffer, *Marymount University, donna.schaeffer@marymount.edu*
Jeree Spicer, *Marymount University, jls54251@marymount.edu*
Patrick Olson, *National University, polson@nu.edu*

Abstract

This paper examines the ethical and legal implications of private sector "hack back" operations in response to cyberattacks. With the Sony incident and the Colonial Pipeline Company incident as the backdrop, we raise issues of cyber defense versus cyber vigilantism. The paper includes discussion of state-sponsored attacks, ransomware, and the societal impacts that result. We discuss the legal aspects of technology in a global context. In the context of cyberattacks, the concept of self-defense raises questions about whether hack back operations can be considered a legitimate form of protection against harm caused by cyberattacks. We address the classification of hack back as a cyber-vigilante action, where individuals or organizations take justice into their own hands without legal authority. We recognize that successful hack back actions require expertise and attribution. Thus, questions arise: Does the victim possess the necessary technical expertise to conduct hack-back operations effectively and safely? Moreover, can the victim, as a practical matter, hack back with a certainty that no uninvolved person is affected?

Keywords: hack back, cybersecurity, cybersecurity law, cyber vigilatism, vigilante, ransomware

Introduction

"Hack back" is a multidisciplinary concept. It has relevance in the fields of cybersecurity, law, criminal justice, and ethics. It describes the actions taken by individuals or private organizations to retaliate against cyberattacks, usually by gaining unauthorized access to the attacker's systems. The term hack-back has been used casually since the early 2000s but gained more prevalence as high-profile cybersecurity incidents, such as the Sony Pictures Corporation and Colonial Pipelines breaches, arose. Today, the term is commonly used. For example, during a House Select Committee on the Chinese Communist Party hearing in March 2025, Representative Raja Krishnamoori (D, IL) said:

> *"I'm going to say something very provocative: I think that we should also consider potentially enlisting private-sector actors to hack back at the hackers. I'm going to get in a lot of trouble for saying that, but I think you have to sometimes use fire against fire (Lovelace, 2025)."*

Hack back is a subject of concept papers and reports published by experts from corporations and think tanks, in the United States and abroad (Ferner, 2024). It is a debate topic e.g., the Back and Forth podcast series asked Should the United States Adopt a 'Hack Back' Cyber Strategy (Center for Strategic and

International Studies, 2025)? For at least a decade, debate has ensued in cybersecurity policy circles, with some advocating for a legal framework that allows defensive tactics and others arguing that, in addition to the fact that hack back is illegal, escalation and attribution errors could cause more harm.

There is no documented information indicating that United States citizens or private organizations have employed hack back tactics in response to breaches. The most notorious incident media associates with the term did not involve any actual hacking back. In 2014, the Guardians of Peace, a hacking group, deployed malware on Sony Pictures Corporation's technology infrastructure. The malware erased important data, disabled key information and communications infrastructure, and leaked sensitive data to the media including emails, legal documents, and unreleased films. The attack was part of an effort to get Sony Pictures Corporation to cancel the release of The Interview, a comedy movie with a plot to assassinate North Korean leader Kim Jong Un.

Sony Pictures business operations were disrupted, its reputation was damaged, and it lost tens of millions of dollars in recovery expenses and employee lawsuits. Following an investigation, the United States Federal Bureau of Investigation attributed the breach to North Korean state-sponsored hackers, although the North Korean government denied any involvement. There were calls for then-President Barack Obama to take aggressive retaliatory actions against the country. However, since it was impossible to attribute the hack to the government of North Korea, he would not act aggressively. He issued an executive order that imposed financial sanctions on countries that sponsor cyber attacks (The White House, 2015) and called for international cooperation in the pursuit of bad actors. Sony Pictures Corporation took only defensive actions in reacting to the breach. They conducted Denial-of-Service attacks on file-sharing servers that made the sensitive and proprietary data available, issued legal take-down notices, and cooperated with the Federal Bureau of Investigation (FBI), the Department of Homeland Security, and other governmental agencies. The company released the film to independent theaters and online streaming platforms.

In May 2021, the concept of hack back returned to the spotlight. Colonial Pipeline's technology infrastructure was breached by Darkside, a criminal gang often attributed to having Russian roots, which compromised its systems. The attack shut down operations and caused fuel shortages across the southeastern United States. Although the company denies hacking back, Colonial Pipeline did pay DarkSide's bitcoin ransomware demands. The company collaborated with the United States Department of Justice and the FBI, which were able to track the bitcoin and seize a portion of the ransomware. This action constituted a lawful search and seizure and followed an unwritten agreement that only the government is authorized to carry out offensive cyber tactics. The incident renewed calls for legislation (LaRue, 2021). Recently, policymakers' attention has shifted from hacking back to improving resilience, public-private cooperation, and funding for cyber defense.

Research Questions

This study aims to explore how cybersecurity literature represents the ethics, risks, and feasibility of hack back as a private-sector cyber defense strategy. It draws on the literature following high-profile incidents, the rise of ransomware-as-a-service, and recent policy debates (e.g., Active Cyber Defense Certainty Act proposals). Our goal is to present two opposing views: hack back as an illegal act or hack back as a form of cyber vigilantism, where individuals or organizations take justice into their own hands without legal authority. This argument raises questions, such as whether the victim possesses the necessary technical expertise to conduct hack back operations effectively and safely, and whether the victim can accurately identify and attribute cyberattacks to the correct attackers, given the complexities and potential for misidentification in cyberspace.

Methodology

This literature review is exploratory, focusing on the topic of hacking back —a retaliatory counteraction taken by individuals or organizations whose information and communication technology systems have been compromised. We searched the Web of Science and IEEE Digital databases using the search terms "cyberattack" or "cyber attack", "cyber vigilantism", and "hack back". This paper extends he work of Bingle and Schaeffer (2021).This is where you introduce the topic of your paper in 11-point Times New Roman font, full-justified. In this example, the topic is to be a guide to help you achieve successful publication of your work in the Issues of Information Systems Journal. The appearance of the *Issues in Information Systems* Journal and IACIS Conference proceedings is greatly enhanced by standardized formatting. Formatting is the same for both Conference and Journal submissions.

Background & Context

Over the past two decades, the evolution of cyber threats has significantly transformed the global security landscape. The increasing complexity and frequency of cyberattacks, mostly ransomware, have exposed the limitations of traditional defensive measures. This ongoing challenge has prompted private-sector organizations to reconsider their cybersecurity strategies, fueling discussions around more assertive responses, including active defense tactics commonly referred to as hack back. Prominent incidents such as the Sony Pictures hack and the Colonial Pipeline ransomware attack demonstrate the growing capabilities of both state-sponsored and criminal cyber actors to disrupt essential services and compromise sensitive data. While these threats are technical, they also carry far-reaching economic, ethical, and societal consequences.

As the scale and impact of cyberattacks continue to escalate, organizations face mounting pressure to consider direct retaliatory actions—even those that may fall outside established legal boundaries. These types of responses fall under the conceptual framework of cyber vigilantism, as defined by Smallridge, Wagner, and Crowl (2016). Cyber vigilantism refers to actions taken by private individuals or entities to impose justice or retribution without legal sanction. It differs from state-authorized cybersecurity operations by involving premeditated, autonomous conduct that may inflict harm while operating outside the formal legal system. Although such behavior is often rooted in frustration over perceived gaps in legal protections or governmental response, cyber vigilantism introduces serious ethical and legal concerns, including risks related to misattribution, disproportionality, and unintended collateral damage.

These developments underscore a growing challenge: private entities are increasingly being drawn into roles traditionally held by governments and law enforcement agencies. When legal responses appear slow or ineffective, some organizations contemplate taking matters into their own hands, an act that closely parallels what scholars refer to as cyber vigilantism. Smallridge et al (2016) present a framework that highlights such actions as typically premeditated, not officially sanctioned, and aimed at punishing or preventing harm. While these actions may seem justified in the context of significant cyber threats, they raise crucial questions: Who determines what constitutes "justice"? What if the wrong target is identified? And what are the implications when harm occurs without legal accountability? These questions are central to understanding the ethical and legal implications of hack-back strategies in the contemporary cyber landscape.

Legal Landscape

In the United States, the Computer Fraud and Abuse Act (CFAA) is the primary federal statute governing unauthorized access to computer systems. Enacted in 1986 and amended multiple times since, the CFAA criminalizes numerous cyber activities, including unauthorized access to protected computers, without exceptions for retaliatory or self-defense actions by private entities (18 U.S.C. § 1030, 2022). This legal gap places organizations in a challenging position: although they face increasingly sophisticated cyber threats, they are prohibited from retaliating even when they can identify the attacker. Internationally, the legal landscape is even less defined. While multilateral agreements, such as the Budapest Convention on Cybercrime, aim to harmonize global laws on cyber offenses, no international treaty or convention explicitly permits or outlines private-sector hack back provisions. Consequently, legal ambiguity persists across jurisdictions, particularly in cross-border incidents where attackers operate in loosely governed cyberspaces.

Smallridge et al. (2016) emphasize the legal and ethical implications of unsanctioned digital retaliation by characterizing it as vigilantism conducted without the authority or oversight of state institutions. Their conceptual model cautions that, despite being motivated by justice or self-defense, such actions typically fall outside accepted legal and social norms. Additionally, challenges in attribution and the potential for collateral damage may inadvertently escalate conflicts or violate laws across multiple jurisdictions. Organizations face challenges in balancing legal compliance with real-time protection due to the lack of updates to frameworks like the CFAA or the absence of explicit policy guidelines. This situation highlights the need for more defined rules of engagement in cyberspace.

Currently, in the United States, hacking back is illegal. The potential of legalizing hack back activities enters popular discussion for brief periods but is then sidelined by other topics; for example, the Active Cyber Defense Certainty Act was first introduced in 2017 by Representatives Tom Graves (R, GA) and Kyrsten Sinema (D, AZ) (H.R. 4036, 115th Congress, 2017). Graves reintroduced a bill in 2019 (H.R.3270, 116th Congress (2019-2020). The bill would have made it legal for victims of persistent cyber intrusions to access the attacker's systems to gather identifying data, destroy stolen data, and monitor the attacker's behavior. The bill never made it out of committee and had languished until recent cyber events, such as the 2025 Salt typhoon attack, a Chinese government-sponsored attack on U.S. telecommunications networks, caused new drafts of bills to emerge.

Ethical Considerations

The ethical debate surrounding hackback operations centers on the distinction between self-defense and vigilantism, two concepts that carry significantly different legal and ethical implications. In traditional physical settings, self-defense refers to an immediate and proportionate response to an unlawful threat, typically sanctioned under national or international law. In contrast, vigilantism occurs when individuals or organizations act outside the scope of legal authority to seek justice or retribution, often driven by frustration, fear, or moral outrage. In cyberspace, this distinction is less clear. As Lin (2016) notes, cyberattacks are often delayed, indirect, and difficult to attribute. The identity of the attacker, the scope of harm, and the legitimacy of a counterstrike are rarely apparent.

Applying principles from just war theory, Lin (2016) argues that hack back operations must meet key ethical criteria: necessity, proportionality, and discrimination. However, these criteria are difficult to satisfy in practice. A private organization's retaliatory cyberattack on a command server could unintentionally disrupt other businesses or critical infrastructure. The risk of misattribution is equally problematic. Cyberattacks are frequently routed through proxy servers or hijacked systems, thereby increasing the likelihood that innocent third parties will be harmed. Without legal oversight or a legitimate chain of authority, such actions may not qualify as self-defense. Instead, they may be better understood as digital vigilantism, with unintended ethical and operational consequences.

Policy Recommendations

Rather than normalizing hack back operations within the private sector, cybersecurity policy should emphasize collaborative governance, coordinated threat intelligence sharing, and proactive defensive strategies. As Palvai (2021) explains, when public institutions fail to respond effectively to cyber incidents, private organizations often feel compelled to act unilaterally. However, allowing non-state actors to launch countermeasures introduces significant legal, diplomatic, and security risks. These unauthorized actions may inadvertently target neutral infrastructure, violate international law, or escalate conflicts with state-affiliated threat actors. Instead of relying on retaliation, governments should expand mechanisms that enable legally sanctioned response pathways and foster strategic partnerships across sectors.

One such mechanism is the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC), which brings together federal agencies, private companies, and international partners to coordinate cyber defense activities. Programs like JCDC are critical for developing joint situational awareness, distributing real-time alerts, and facilitating cooperative incident response. However, participation should be expanded to include small and mid-sized enterprises that may lack the capacity to act independently. These organizations often experience cyberattacks but lack access to the same resources and intelligence as large corporations. Policy should encourage tiered public-private response models that allocate resources, support, and authority in proportion to risk exposure and sector criticality.

The No Hacking Back guide by Cybersecurity Tech Accord (n.d.) emphasizes effective alternatives to offensive tactics. Examples include deploying honeypots to deceive and monitor adversaries, adopting a zero-trust architecture to prevent internal compromise, and utilizing automated segmentation and containment technologies to neutralize attacks in real-time. Additionally, information-sharing initiatives, such as Information Sharing and Analysis Centers (ISACs), enable the secure dissemination of threat intelligence across industries. Governments can further incentivize best practices by offering tax credits, regulatory relief, or procurement preferences to organizations that meet cybersecurity maturity benchmarks. In this way, policy can shift the focus from retaliation to resilience, empowering organizations to act confidently within a defined legal and ethical framework.

Conclusion

The question of whether hack back operations should be allowed or encouraged extends beyond legal boundaries and technical feasibility. It is also a psychological issue, shaped by emotion, urgency, and a perceived failure of justice. Angela, Aulia, and Rahma (2020) examine how digital vigilantism arises in environments where formal institutions are perceived as ineffective or absent. Emotional drivers—such as anger, fear, or the need to restore a sense of control often influence decisions more than legal rationale or strategic outcomes. These dynamics are particularly relevant in cybersecurity, where the aftermath of a breach often includes reputational damage, operational disruption, and pressure from stakeholders to respond decisively. In such situations, organizations may feel tempted to retaliate rather than rely on law enforcement or government support.

Hack back operations offer the illusion of empowerment, but they present significant long-term risks. Uncoordinated cyber retaliation can compromise global stability, lead to unintended diplomatic consequences, and erode public confidence in the rule of law and due process. This is especially dangerous when private-sector actors misattribute an attack or act disproportionately to the threat, potentially escalating tensions with nation-states or criminal networks. Even well-intentioned actions can result in data loss, infrastructure damage, or harm to innocent users if countermeasures are not precisely targeted and legally authorized.

The way forward lies in fostering collaborative and accountable cybersecurity ecosystems. Governments must take the lead in defining clear legal boundaries, establishing response protocols, and investing in national and cross-border cyber resilience infrastructure. At the same time, the private sector should be supported in adopting best-in-class defensive practices, contributing to threat intelligence initiatives, and

participating in joint readiness exercises. Civil society also plays a role by promoting transparency, ethical standards, and the human rights implications of digital defense. Together, these stakeholders can shift the focus from reaction to prevention, strengthening cyber defense while preserving legal norms and the psychological balance needed to make the digital world safer for all.

Acknowledgements

Dr. Schaeffer and Dr. Spicer acknowledge the support from Marymount University Summer Research Fellows program. GrammarlyTM was used for spelling and grammar review.

References

18 U.S.C. § 1030. (2022). Computer Fraud and Abuse Act. Cornell Law School Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1030

Angela, L., Aulia, W., & Rahma, B. G. J. S. (2020). "No viral, no justice": Unveiling the phenomenon of digital vigilantism from a psychological perspective. Faculty of Psychology, Universitas Gadjah Mada. https://vc.bridgew.edu/ijcic/vol3/iss1/3/

Center for Strategic and International Studies. (2025, April 24). Back & Forth 4: Should the United States Adopt a "Hack-Back" Cyber Strategy? Retrieved from CSIS: https://www.csis.org/analysis/back-forth-4-should-united-states-adopt-hack-back-cyber-strategy

Cybersecurity Tech Accord. (n.d.). No hacking back: Vigilante justice vs. good security online — A policymaker's guide to knowing the difference. https://www.cybertechaccord.org/no-hacking-back/

Ferner, J. (2024, September 18). Current Overview of Hackbacks in Germany: Political Debates, Legal Status, and Planned Legislation. Retrieved from German lawyer Ferner: https://www.ferner-alsdorf.com/current-overview-of-hackbacks-in-germany-political-debates-legal-status-and-planned-legislation/

H.R.3270 - 116th Congress (2019-2020): Active Cyber Defense Certainty Act. (2019, June 28). https://www.congress.gov/bill/116th-congress/house-bill/3270/text

La Rue, H. A. (2021). Outsourcing the Cyber Kill Chain: Reinforcing the Cyber Mission Force and Allowing Increased Contractor Support of Cyber Operations. *J. Nat'l Sec. L. & Pol'y*, 12, 583.

Lin, P. (2016). Ethics of Hacking Back: Six Arguments from armed conflict to zombies. *Available at SSRN 4682398*.

Lovelace, R. (2025, March 05). Momentum builds on Capitol Hill to approve private sector hack-back against China. *The Washington Times.*

Palvai, R. (2021). Internet vigilantism, ethics and democracy. Department of Communication and Journalism, Osmania University. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3938264

Smallridge, J., Wagner, P., & Crowl, J. N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology*, 8(1), 57–70.

The White House. (2015, April 1). Executive Order 19634. Retrieved from Obama White House Archives: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m