Is it ethically justifiable for a victimized organization to engage in retaliatory hacking, commonly known as 'hack back'?

Hayden Vermeulen

Old Dominion University

IDS-300W

Dr. Pete Baker

12/8/23

Is it ethically justifiable for a victimized organization to engage in retaliatory hacking, commonly known as 'hack back'?

In recent years, the whole realm of cybersecurity and ethics has really taken center stage. People are starting to wonder if it's okay for organizations that have fallen victim to cyberattacks to hit back in what's commonly known as 'hack back.' It's a real head-scratcher when you think about it. Kristian Gerke (Gerke, 2023) had something interesting to say about this in 2023. She shared this story about Shawn Carpenter, a cybersecurity whiz, who back in 2003 tracked down a cyberattack all the way to a server in China. Carpenter wasn't just focused on his own ideal's, he told the FBI about the cyberattack. Surprisingly, the FBI not only welcomed his help but also used the intel he provided to take things further. Carpenter got fired from his job at Sandia National Laboratories for exposing these findings. They claimed he broke the law. He took them to court, fought for what he believed was right, which the court found not guilty. So, this whole thing got me thinking. What's the deal with victimized organizations playing the hacking game themselves? It's like a digital Wild West out there, and as tech keeps evolving, it's making us question the ethics of fighting fire with fire in the cyber world. It's not just about bits and bytes; there's a real moral tug-of-war happening, and the 'hack back' debate is right at the heart of it.

Interdisciplinary Justification

An interdisciplinary approach proves indispensable in justifying the exploration of the ethical dimensions surrounding victimized organizations engaging in retaliatory hacking, colloquially termed 'hack back.' The landscape of cybersecurity is inherently complex, intertwining technological, legal, ethical, and societal dimensions. By adopting an

interdisciplinary perspective, we open avenues to draw insights from diverse fields, fostering a more comprehensive understanding of the intricate issues surrounding retaliatory hacking.

Ethical considerations are at the crux of the 'hack back' debate, requiring input from ethics and philosophy to delve into the moral implications of such actions. This involves a nuanced assessment of the rights and responsibilities of organizations, potential collateral damage, and the ethical frameworks guiding cyber activities. Examining the societal perspective reveals that the impact of cyber activities extends beyond individual organizations to society at large. A sociological lens, afforded by an interdisciplinary approach, facilitates a deeper understanding of societal implications, including the potential for escalation and the broader consequences of 'hack back' practices. Crafting effective cybersecurity policies and governance frameworks necessitates the involvement of multiple disciplines. Political science, psychology, and economic experts contribute to shaping regulations and guidelines surrounding 'hack back' activities, ensuring a balanced and ethical approach.

In the landscape of cybersecurity, political science serves as a guiding force, unraveling the geopolitical intricacies that underlie cyber conflicts and shaping global strategies. Psychology, a cornerstone in understanding the human side of the equation, peels back the layers to reveal the motivations driving cyber threat actors, influencing the development of defenses centered around users and fostering cybersecurity awareness. Economics, adopting a pragmatic lens, assesses the economic dimensions through cost-benefit analyses of cybersecurity investments and a critical examination of the economic fallout from cyber incidents. Together, these disciplines form a powerful alliance, providing a holistic understanding of the intricate challenges in cybersecurity, offering a robust foundation to tackle the complexities of cyber

threats. This collaborative effort not only equips us to navigate the ever-shifting digital terrain but also empowers the formulation of effective strategies to fortify our cyber domains.

Literature Search

When evaluating Canada's engagement in active cyber defense from a political science perspective, the intricate ethical considerations further amplify the complexity of the analysis. Determining the ethical implications of Canada's potential involvement in hack back activities requires a nuanced examination, considering the inherent challenges such as potential collateral damage, attribution uncertainties, and the risk of escalating cyber conflicts.

Ethical assessments in the context of Canada's active cyber defense efforts become particularly salient, given the nation's commitment to international norms, legal frameworks, and diplomatic principles. The challenge lies in striking a delicate balance between the imperative to protect national interests and upholding ethical standards (Gerke, 2023.) The ethical dimension introduces subjectivity, making it challenging to establish a universally accepted framework for evaluating the morality of hack back actions.

Engaging in hack back activities with other nations introduces a complex interplay of diplomacy, ethics, law, and strategy. Diplomatically, such actions can strain international relations and impede collaborative efforts in the realm of cybersecurity. Effective diplomacy requires a delicate balance between asserting national interests and fostering global cooperation. Ethical considerations loom large, given the potential for collateral damage and misattribution in the unpredictable landscape of offensive cyber operations.Kallberg looked into international cooperation and dialogue emerging as critical components in addressing the multifaceted challenges associated with hack back activities between nations (Kallberg, 2016.) The

establishment of norms, treaties, and confidence-building measures is imperative to foster stability and security in cyberspace. Political scientists, with their interdisciplinary expertise, play a pivotal role in analyzing the impact of hack back actions on global dynamics, diplomatic relations, and the evolution of norms governing state behavior in the ever-changing cyber landscape. Collaborative efforts at both national and international levels are essential to navigate this intricate terrain and ensure responsible behavior in the increasingly interconnected world of cyberspace (Gerke, 2023.)

The psychological discipline brings perspective to the realm of hack back activities, offering insights into the motivations that propel individuals or groups to engage in offensive cyber operations. Examining the intricate web of political ideologies, hacktivist principles, or personal grievances that drive these actions allows for a deeper understanding of the human factors shaping cyber conflict. Marcelo claimed that 60% people have influence from emotional factors when deciding to hack back as retaliation (Marcelo M Leal, 2022.) By unraveling the complexities of the psychological drivers, psychologists contribute to a more comprehensive analysis of hack back activities, shedding light on the intricate motivations that underpin offensive cyber behavior.

Beyond motivations, psychology plays a crucial role in assessing the impact of hack back activities on both the perpetrators and potential victims. Engaging in offensive cyber operations can evoke a spectrum of emotions, from a sense of empowerment or vindication for those conducting the attacks to anxiety and fear for the entities being targeted (Musgrave, 2022.) The psychological toll of cyber conflicts extends beyond the digital realm, influencing individuals and societies. Analyzing these psychological repercussions provides valuable insights into the broader implications of hack back strategies, helping to navigate the human dimensions of cyber warfare.

The discipline of psychology is instrumental in understanding the tactical aspects of hack back operations. Social engineering, manipulation techniques, and the exploitation of cognitive biases are prevalent in offensive cyber activities. By unraveling the psychological principles at play, psychologists contribute to the development of effective countermeasures and cybersecurity strategies throughout the world. (McGuigan, 2019.) This understanding is pivotal in enhancing awareness and resilience against the psychological tactics employed in the dynamic landscape of cybersecurity.

The economic discipline provides valuable insights into the motivations and consequences of hack back activities. Economists contribute by examining the cost-benefit analyses associated with offensive cyber operations, exploring the financial incentives that drive both state and non-state actors to engage in cyber conflicts. This economic perspective delves into the expenses incurred in developing advanced cyber capabilities, potential gains from stolen data, and the economic impact of cyber incidents on targeted entities (Nobles, 2023.) By integrating economic considerations into interdisciplinary frameworks, we gain a more comprehensive understanding of the rationality behind decisions to embark on hack back strategies, enriching our analysis of cyber conflicts. Economic concepts contribute to unraveling the dynamics of the cybercrime market, operating on principles of supply and demand. Recognizing the interconnected nature of cybersecurity challenges, this interdisciplinary lens, which includes economic considerations, deepens our comprehension of the economic dimensions influencing hack back operations and their repercussions on a global scale.

Hack back activities conflict viewpoints within the economic discipline revolve around the rationality of engaging in offensive cyber operations. While proponents argue that financial incentives, potential gains from stolen data, and the economic impact on targeted entities justify such strategies, opponents contend that the long-term economic repercussions outweigh any short-term gains.

Ethical considerations add another layer of conflict, particularly within the discipline of political science, as Canada evaluates its potential involvement in active cyber defense. The debate centers on determining the ethical implications, with tensions arising between safeguarding national interests and adhering to ethical standards. Factors such as potential collateral damage, attribution uncertainties, and the risk of escalating cyber conflicts intensify the ethical dilemma, sparking debates on the appropriate course of action.

Psychological discipline perspectives bring conflicts regarding the motivations behind hack back activities. Some emphasize political ideologies and personal grievances as primary drivers, while others argue that emotional factors, such as frustration or the desire for retaliation, may play a more significant role. This conflicting insight introduces a layer of uncertainty, underscoring the challenge of establishing a definitive understanding of the human factors influencing offensive cyber behavior. The psychological landscape of hack back activities remains complex, with diverse viewpoints shaping the discourse on the motivations behind such actions.

Common Ground

In the scattered diverse space of hack back activities, divergent economic perspectives prompt an exploration of the rationale behind offensive cyber operations. Advocates posit that financial gains, potential data rewards, and impacts on targeted entities justify such strategies, while critics argue that the potential long-term economic repercussions outweigh immediate benefits. However, common ground emerges as both sides share a fundamental concern for national security, recognizing the imperative of securing the nation's interests. Ethical considerations, particularly within political science, introduce an additional layer of conflict, with debates centering on the ethical implications of nations like Canada engaging in active cyber defense. Tensions arise between safeguarding national interests and adhering to ethical standards, emphasizing the need for responsible cyber practices. This shared advocacy for

responsibility becomes a unifying factor amid ethical debates. In the psychological domain, conflicting perspectives on motivations behind hack back activities unfold, ranging from political ideologies to emotional factors. Despite this diversity, a shared emphasis on cybersecurity innovation and defense becomes a potential meeting point, underlining the importance of investing in defensive measures and technological advancements to navigate the intricate complexities of cyber threats collaboratively.

A unique insight emerges: the imperative to integrate diverse perspectives for a comprehensive understanding. Amidst economic debates surrounding offensive cyber operations, the careful consideration of short-term gains versus long-term repercussions is not just a financial dilemma but a strategic balancing act. Recognizing the shared concern for national security serves as a unifying touchpoint, transcending economic differences. Ethical considerations, often centering on responsible cyber practices, offer not just a guideline but a common ethical ground that can foster collaborative decision-making. In the realm of psychology, the varied motivations behind hack back activities underscore the necessity for a nuanced approach. Uniquely, the emphasis on cybersecurity innovation and defense emerges not merely as a technological strategy but as a collective commitment to resilience. Integrating these insights, therefore, goes beyond understanding; it becomes a synergistic process that empowers stakeholders to forge a more united and effective response to the multifaceted challenges inherent in hack back activities.

Organizing interdisciplinary workshops or roundtable discussions would provide a platform for stakeholders to communicate their insights, drawing from economic analyses, ethical considerations, and psychological understandings. This exchange of ideas can be a valuable testing ground for the proposed insight, allowing for refinement based on real-world experiences and diverse viewpoints. Practical simulations or tabletop exercises involving professionals from different disciplines can be conducted. These simulations would create scenarios related to hack back activities, enabling participants to apply the integrated insights in

a controlled environment. Through these exercises, the efficacy of the comprehensive understanding in guiding decision-making and responses to cyber threats can help lower potential ‘hack back’ attacks.

Work Cite:

Gerke, K. (2023). Canadian hack-back?: A consideration of the Canadian legal framework for private-sector active Cyber Defence. Alberta Law Review. https://albertalawreview.com/index.php/ALR/article/view/2668

Kallberg, J. (2016). A right to Cybercounter strikes: The risks of legalizing Hack Backs ... https://ieeexplore.ieee.org/document/7030161/

Leal, M. M., & Musgrave, P. (2022). Hitting back or holding back in Cyberspace: Experimental evidence ... https://journals.sagepub.com/doi/10.1177/07388942221111069

McGuigan , A. S. (2019). Hacking back: Justifiable or vigilantism - proquest. https://www.proquest.com/docview/2316055855/previewPDF?fromunauthdoc=true

Nobles , C. (2023). A Scoping Review of Hacking Back in Cybersecurity. AIS eLibrary. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1022&context=mwais2023