On the Offensive

Gavin L. Williams

Old Dominion University

IDS300W: Interdisciplinary Theory and Concepts

Dr. Kat Lafever

November 21, 2023

Abstract

With the ever-evolving landscape of cybersecurity, the line between hackers and defenders has grown ever less clear. Many cybersecurity specialists started their careers off the backbone of offensive or criminal techniques. They are taught how to use the tools of the criminals to understand and protect against such attacks. However, it is becoming more apparent that the defending side may no longer be able to keep up with the clever minds of the attackers. With this in play, what can be done for the righteous to prevail? Just as swiftly as hackers uncover new vulnerabilities, our experts must discover contemporary strategies. Considering this, what more effective strategy could there be than to combat fire with fire itself? Who knows how hackers think better than fellow hackers, who knows common vulnerabilities greater than those who exploit them, and who knows how to bring a company down more than someone who has? This research addresses the question; what are black-hat and red-hat hackers, and why are companies hiring them to hack-back as grey-hat hackers? As well as the risk and ethics to be considered with this approach to cybersecurity.

Keywords: red-hat hacking, black-hat, grey-hat hacking, implied trust, ethical hacking, offensive cyberactivities, and legal framework.

On The Offensive

As time moves on, the escalating reliance on technology has made the need for enhanced digital security more apparent than ever. Bad actors have become an ever-increasing threat to our society, necessitating the investigation of alternative approaches to further enhance our cybersecurity measures. I propose we explore the questions: what are black-hat and red-hat hackers, and why are companies hiring them to hack-back as grey-hat hackers? Is this considered an ethical approach? This research draws on multiple different disciplines involving aspects of computer science, ethics, and psychology. When investigating the characteristics, motivations, and practices of red-hat and grey-hat hackers, disciplines such as computer science and cybersecurity expertise are needed to understand their technical skills, while knowledge in psychology can shed light on their motivations and behaviors. Additionally, we can draw on conclusions from ethical studies to assess whether this approach aligns with ethical norms. An interdisciplinary approach is essential for this research for examining the complex aspects of red-hat hackers, grey-hat hacking and the ethical implications of companies hiring hackers to hack back as ethical hackers. It is important that we draw from various fields of expertise to understand the implications at play from more than just a technical point of view. The findings from this research will be highly beneficial in relation to my major in cybersecurity. Furthermore, I intend to include this work in my academic portfolio to showcase my scholarly pursuits.

Black, White, Red, and Grey-hat Hacking

This section defines key terms such as white-hat, black-hat, red-hat, and grey-hat hacking. *White-hat hacking* according to Kapadia, Kundalia, and Kanade (2020), Computer Science scholars from Ahmedabad University, is the legal and ethical form of hacking while *black-hat hacking* refers to the practice of exploiting vulnerabilities within a computer system or network for malicious purposes, and those who engage in this form of cyber activity are known as black-hat hackers (Kapadia, Kundalia, & Kanade, 2020, p. 2). There are many motivations for some to turn to black-hat hacking. The number one

motivator being financial gain, and with the growing societal reliance on technology cybercrime has become an attractive alternative to physical crime. Other motives for black-hat hacking can range from political activism to simple amusement, some individuals find the challenge of breaching secure environments to be exciting and commit these acts for enjoyment. Regardless of their motivations the actions of black hat hackers pose significant risks to individuals, businesses, and even national security. As such, these individuals are deemed criminals in the eyes of the law, and the attacks they commit are strenuously opposed by cybersecurity specialists across the world. This constant game of offense versus defense between hackers and cybersecurity experts is what shapes the evolving landscape of cyber defense strategies.

Red-hat hackers as defined by Withers et al. (2020), who are professors of Cybersecurity at Nova Southeastern University, are individuals "who use hacking techniques to perform their job functions. (This is as opposed to "white-hat" hackers, who work primarily defensively, and "blackhat" hackers, who act maliciously). Red hats are considered the vigilantes of the hacker community when responding to cyber attribution" (Withers et al. 2020, p.1814). Red-hat hackers are skilled individuals that locate vulnerabilities used by black-hat hackers. However, unlike a standard security professional, rather than reporting the weakness or fixing the issues they take an alternative approach to stopping the bad actor. A red-hat hacker will use their technical expertise to take down the offending system or attack the infrastructure used by the black-hat hacker, and in doing so prevent them from causing further harm. This operation is called a "*hack-back*" because rather than defending against the attack, they hack back the attackers.

Grey-hat hacking is a combination of white-hat hacking and black-hat hacking. A *grey-hat hacker* as described by Pratibha (2019), an information technology assistant professor at D.B.J. College, is a computer hacker or security expert who may sometimes violate laws or ethical standards, but not with malicious intent. These individuals may exploit vulnerabilities for personal gain and sometimes disclose

these vulnerabilities to the affected parties or the public, often operating for the common good. An example of grey-hat hacking would be an individual finding an exploit within a company's systems, and then rather than reporting the issue they offer to repair it in exchange for money (Pratibha, 2019, p. 1089). For this research the ethical dilemma for grey-hat hacking relates to how far to one side they may act. For instance, if they operate more in line with a black-hat hacker it could become dangerous for the company.

Computer Science Disciplinary Research

When considering the employment of hackers as cybersecurity professionals for conducting offensive operations as well as for enhancing overall security measures, it is critical to assess the results and challenges this presents from a technical standpoint. As Withers et al. (2020) explains "Offense involves exploiting systems, penetrating systems with cyber-attacks, and generally leveraging broken software to compromise entire systems and systems of systems [32]. Conversely, defense means building secure software, designing, and engineering systems to be secure in the first place, and creating incentives and rewards for systems that are built to be secure [33]. Ultimately, offensive security is a proactive and adversarial approach to protecting computer systems, networks, and individuals from attacks" (Withers et al. 2020, p. 1814). Many cybersecurity teams are too focused on just the defensive side of security and completely ignore any offensive strategies. The idea is if their defense is strong enough then nothing else matters. Yet experience consistently shows that the adversaries are resourceful, and given sufficient time, they will inevitably discover a vulnerability to exploit. As it shows, many adversaries have technical knowledge of computer systems and vulnerabilities; thus, it would greatly benefit the advancement of cybersecurity to offer ethical work to these individuals. They could work as grey-hat hackers in projects to either lawfully hack into the computer systems to relay information and suggest solutions or work to find and potentially stop those attacking our own systems. Hiring hackers to work in cybersecurity operations has been done before, as for example in Kapadia,

Kundalia, and Kanade's (2020) research explains how "Hackers who are considered worthy of a second chance by authorities are employed by 'Bluescreen', a cyber-security company in Plymouth. They work with the *police against other hackers who they earlier used to see as their fellow brothers" (Kapadia, Kundalia, &* Kanade, 2020, p. 4). This arrangement proves advantageous for both parties, providing the company with skilled specialists while offering formerly directionless hackers an opportunity to apply their skills towards a positive purpose. While offensive cyber operations are less common on a civil scale there are plenty of instances of offensive cyber attacks on a national level. As Withers et al. (2020) explain within their research the "U.S. intelligence agencies initiated 231 offensive cyber operations in 2011, nearly threequarters of them against key targets such as Iran, Russia, China, and North Korea, some intended to disrupt nuclear proliferation" (Withers et al. 2020, p. 1814). One could debate the ethics of these attacks; however, on a national scale, they are often considered essential to the well-being of the country.

Psychological Disciplinary Research

Ethical Hacking as a practice requires a deep understanding of the psychology behind both hacking and defense. Ethical hackers must be able to understand the mindset of their adversaries by employing the same creative thinking and problem-solving skills to counteract threats. A cybersecurity specialist faces complex evolving challenges and must maintain composure and persistence in the face of repeated setbacks. Numerous specialists dedicate themselves to exhaustive studies to understand the technical strategies employed by attackers. However, it is equally important for a specialist to possess empathy and the ability to see things from others' perspectives. This deeper understanding of the opposition's thought process is crucial. Repko and Szostak (2021) state, "multicausal integration sees changes in the subject phenomenon as the outcome of several different interdependent variables" (p. 337). This means that several distinct factors combine to produce a specific result, and this result is linked to another outcome. I can apply this strategy to my research because multiple factors can lead an

individual to become either a malicious hacker and, consequently, be employed as an ethical hacker. For instance, factors like a person's financial situation, upbringing, and psychological conditions can increase their likelihood of turning to cybercrime. Furthermore, the growing societal reliance on technology has made cybercrime an attractive alternative to physical crime. These combined factors can motivate someone toward becoming a black-hat or red-hat hacker. With the increasing amount of cybercrime, it is crucial to explore additional solutions for strengthening information security. One potential solution involves adopting an offensive approach, in which malicious hackers or red-hat hackers are hired to hack back other hackers as grey-hat hackers. From a psychological perspective, these hackers are equipped not just with the necessary skills, but also with the mindset of a hacker. This positions them ideally to understand what is needed to safeguard systems against bad actors. Additionally, they have the capability to proactively target and neutralize hackers who pose a threat to our systems.

Ethical Disciplinary Research

Grey-hat hacking occupies a unique and often controversial space in the world of cybersecurity. It represents a middle ground between ethical white hat and malicious black hat hacking. While grey hat hacking contributes to improving security by uncovering flaws in a system, it does so at the cost of bypassing consent and legal boundaries. Moreover, it is usually in the hopes of financial gain rather than for the good of the company. Ethical research typically involves organizing, justifying, and advocating for principles of what is considered morally correct and incorrect actions. For this research we will be looking at virtue ethics specifically. As Withers et al. (2020) explain, “Virtue ethics are currently one of three major approaches in normative ethics. In it, virtues are values behind ethical actions or principles behind codes of conduct, moral properties that people use to act ethically. Human nature, social norms, and workplace culture generally pull one toward virtues.” (Withers et al. 2020, p. 1816). Using this approach Withers and his colleagues were able to construct a survey to see if offensive hack back operations were deemed ethical. The result showed that “the majority do not find it unethical to “hack

back” adversaries in nation-states and that private companies should be given the right to retaliate without prosecution” (Withers et al. 2020, p. 1819). Looking ahead, it is important to address the ethical issue involved in employing former malicious hackers as ethical hackers. For instance, should these offenders be given a second opportunity, and can their past misconduct be disregarded due to their expertise? Typically, this is viewed as an ethical strategy; nonetheless, it carries a risk to assign such individuals roles of responsibility where they might potentially inflict damage. George, Oliver, and Gregory (2018), PhD scholars in the field of information technology at Charles Sturt University, explain how "Because of the implied trust relationship between an ethical hacker and the client, the ethical hacker is at an advantageous position and effectively given permission to access any information they can, much of which could be confidential or sensitive in nature" (George, Oliver, and Gregory 2018, p. 15). Entrusting such sensitive information to these individuals may pose challenges in preserving security.

Creating Common Ground

There are three major findings disclosed by this interdisciplinary research. First, the critical role of technical expertise, as cybersecurity is a multifaceted study involving a high level of technical knowledge and problem-solving skills. Therefore, it is beneficial to broaden our pool of potential candidates for cybersecurity specialist roles, regardless of the individuals' backgrounds. However, this leads us into our next major finding regarding the psychology of the individuals we choose to employ. For this research, we are discussing the implications of hiring past criminals to work with highly sensitive data and important systems. It was made clear that those in question have a low moral compass; moreover, in the case of hiring red-hat hackers while not as polarizing as black-hat hackers they still generally have very stark motivations that strive away from what one should expect from a cybersecurity specialist. Lastly, we need to highlight the ethical and legal implications of hack-back strategies. Although these strategies can provide proactive defense against cyber threats, they also risk violating legal boundaries

and ethical norms, potentially causing unintended harm or escalating conflicts. These offensive operations often do not have clear legal guidelines or codes of conduct, making these actions a question of ethical practice. While many people find this to be a justifiable approach it is not unanimously agreed upon. It is important to find common ground between these major disciplines to arrive at any notable conclusions. The main points of similarity lie with the need for technically gifted individuals and how psychologically looking past moral dilemmas those who work against us are the perfect candidates to work alongside us to better cybersecurity as a practice. However, we find most issues when looking at this ethically, as the people in question are criminals and it may not be ethically sound to allow them a second chance. Moreover, using them in offensive often illegal activities for the benefit of a company or large entity causes controversy over the ethical implications. Creating common ground is imperative for this research as it allows for integrative thinking. This approach, as Repko and Szostak (2021) state, “We do not consciously reflect on all the components of such decisions because of our natural capacity to process information” (p. 270). One person or in this case, one discipline can only provide so much information; therefore, we are unable to gather information regarding every aspect of the problem. Thus, we must combine the thinking of multiple different disciplines to broaden our range of information to cover most if not all aspects surrounding the problem. This and the ability to solve complex questions such as this one using insights from multiple fields of study cumulatively, are why interdisciplinary research is such a powerful tool in advancing our understanding and addressing multifaceted challenges.

Underlying Conflicts and Understandings

One significant conflict lies between the psychological understanding of hacker motivations and the ethical implications of their actions. Psychological research suggests that hackers, regardless of their 'hat' color, often act based on a complex mix of personal motivations, which can include thrill-seeking, a sense of justice, or financial gain. However, from an ethical standpoint, these motivations can conflict

with normative principles about right and wrong, especially in the context of grey-hat hackers employed by companies for hack-back operations. While psychology might explain and even justify certain behaviors based on underlying motivations, ethics raises questions about the moral legitimacy of these actions, particularly in cases where legal boundaries are blurred or crossed. Additionally, as mentioned above, there are the issues present between cybersecurity strategies and ethical considerations. It is important to mention that while cybersecurity experts may argue for the effectiveness of such strategies in deterring or responding to cyber threats, ethics experts might challenge the moral implications and potential for unintended consequences. To bridge these differences, an interdisciplinary approach is required, one that combines ethical reasoning into the psychological profiling of hackers and the development of cybersecurity strategies. This could involve integrating ethical expertise into cybersecurity codes of conduct and procedures. By fostering communications between experts in each field of study we can develop strategic decisions that align with multiple ways of thinking and practice.

Constructing a More Comprehensive Understanding or Theory

In recent years, there has been a significant shift in corporate strategies, integrating new approaches that often intersect with ethical and legal considerations. To effectively integrate the previously mentioned cyber strategies, it is essential to develop and implement systems aimed at normalizing these approaches. Most of the issues relating to ethical and legal complications are due to the relatively new incorporation of this strategy in corporate settings. Bearing this in mind, many individuals will be more likely to agree that an action is ethically acceptable if it is both common and legal. Additionally, there is peace of mind if this is viewed from the perspectives of professionals from various fields of study relating to the issue, collaborating to formulate a code of conduct or another strategy to systematize this approach. Moreover, the risk associated with employing individuals based solely on their technical skills, especially those with questionable backgrounds, can be mitigated. This can be achieved by implementing contingency plans that limit the extent of control or influence these

individuals have within the organization. By doing so, companies can leverage their technical abilities while safeguarding against potential ethical or legal transgressions.

Reflecting On, Testing, and Communicating the Understanding or Theory

To test the outcome of implementing this cyber strategy, we will need to work constructively to establish a plan, enabling us to discern what is effective and what is not. We should then continually adjust and enhance various elements to remain aligned with current and future trends and threats in the cyber landscape. Future research on this subject would benefit from looking into the legal and sociological aspects of these approaches. Legal research will be necessary to ensure compliance with evolving regulations and to understand the broader legal implications of our strategies in various jurisdictions. Exploring sociology can reveal the outcomes of inviting hackers to serve as cybersecurity experts, along with the potential societal consequences this practice may bring about. Finally, when assessing ethical perspectives on this topic, obtaining meaningful results from surveys appears challenging. This difficulty arises because many test subjects already hold established views on cyber practices, and there is a noticeable trend of male predominance in the sample size, reflecting the gender disparity often seen in computer science.

Conclusion

In conclusion, this research has explored the intricate and often controversial connections of cybersecurity, ethics, and psychology through the lens of employing hackers for defensive and offensive cyber strategies. It highlights the technical prowess and unique insights that hackers, particularly those with red-hat and grey-hat backgrounds, can bring to the cybersecurity domain. However, it also underlines the ethical and legal challenges present in such approaches, particularly when it comes to employing individuals with a history of malicious activities. While the integration of these hackers into cybersecurity roles can enhance security strategies against cyber threats, it is imperative to develop robust ethical guidelines and legal frameworks to govern such practices. To do so, it is crucial to create

common ground between relevant disciplines, as well as ensuring diversity and inclusivity in research and practical applications. Ultimately, this research calls for an interdisciplinary approach, combining technical, psychological, and ethical perspectives, to explore the potential of employing hackers in cybersecurity while mitigating the risks and moral dilemmas associated with such strategies. This comprehensive view is essential for advancing the field of cybersecurity in a manner that is effective, responsible, and aligned with ethical values and legal standards.

References

Georg, T., Oliver, B., & Gregory, L. (2018). Issues of implied trust in ethical hacking. *The Orbit Journal*, *2*(1), 1–19. https://doi.org/10.29297/orbit.v2i1.77

Jumale, Pratibha. (2019). Impact of Ethical Hacking on Business and Governments. *International Research Journal of engineering and technology*, *6*(12). https://www.irjet.net/archives/V6/i12/IRJET-V6I12177.pdf

Kapadia, Udit & Kundalia, Samkit & Kanade, Meghna. (2020). Grey hat hacking: normative ethical theories-based opinion piece/report. *Researchgate Publication.* https://www.researchgate.net/publication/341270737_GREY_HAT_HACKING_Normative_Ethical_Theories-based_Opinion_PieceReport

Munjal, Meenaakshi. (2014). Ethical hacking: an impact on society. *Cyber Times International Journal of Technology and Management,* 7, 922-931. https://www.researchgate.net/publication/262726769_ETHICAL_HACKING_AN_IMPACT_ON_SOCIETY

Repko, A. F. & Szostak, R. (2021). Interdisciplinary research: Process and theory (4th ed.). SAGE Publications, Inc.

Withers, K., Parrish, J., Ellis, T., & Smith, J. (2020). Vice or virtue? exploring the dichotomy of an offensive security engineer and government “hack back” policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1813–1822. https://doi.org/10.24251/hicss.2020.224