Vice or Virtue? Exploring the Dichotomy of an Offensive Security Engineer and Government "Hack Back" Policies

Kim L. Withers
Nova Southeastern University
kw954@mynsu.nova.edu

James L. Parrish
University of North Texas
james.parrish@unt.edu

James N. Smith
Augusta University
jasmith8@augusta.edu

Timothy J. Ellis
Nova Southeastern University
ellist@nova.edu

Abstract

In response to increasing cybersecurity threats, government and private agencies have increasingly hired offensive security experts: "red-hat" hackers. They differ from the better-known "white-hat" hackers in applying the methods of cybercriminals against cybercriminals and counter or preemptively attacking, rather than focusing on defending against attacks. Often considered the vigilantes of the hacker ecosystem, they work under the same rules as would be hackers, attackers, hacktivists, organized cyber-criminals, and state-sponsored attackers—which can easily lead them into the unethical practices often associated with such groups. Utilizing the virtue (ethics) theory and cyber attribution, we argue that there exists a dichotomy among offensive security engineers, one that appreciates organizational security practices, but at the same time violates ethics in how to retaliate against a malicious attacker.

1. Introduction

Currently, there is a hacker attack every 39 seconds, affecting one in three Americans each year [10]. As the Internet penetrates more deeply into people's daily lives, the vectors of attack for cybercriminals and hackers will continue to multiply, and, as Internet use continues to expand, the total number of cyber-attacks grows annually and the potential damage from cyber-attacks also increases. According to Gartner, the consistent rise of cybercrime has amplified information security spending to more than $86.4 billion in 2017 [36]. That value does not include an accounting of the Internet of Things (IoT), industrial control systems (ICS), automotive security, and other cybersecurity categories. According to a Cryptologic Program budget analysis, the intelligence community invested roughly one-third of the total cyber-operations budget of roughly $1.02 billion on defense of military and other classified computer networks against foreign attacks in fiscal year 2013 [17]. Though economic calculations vary extensively and are difficult to make, cybercrime and data loss have been estimated to cost the global economy at least $1 trillion annually [12]. A generalized definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both" (as cited in [5], p. 141). But those who commit cybercrimes may have different motivations from those who initiate cyber-attacks.

Cyber-attacks have the potential to cause substantial and wide-ranging harm across a number of critical arenas. These targeted attacks against nuclear infrastructure, such as Stuxnet [6]; attacks against commercial entities, such as the Sony hack [19]; attacks against government infrastructure, such as the Estonia DDoS attack [37]; and attacks against political entities, such as the Democratic National Committee (DNC) hack [23]. Cutting-edge spyware or malware is likely to be found on the computers of senior government officials or on important network systems within national critical infrastructures. Governments, corporations, and individuals have prudently responded to these cybercrime trends by hardening their cyber defenses. For instance, shortly after the Sony Pictures hacks, the United States and the United Kingdom announced a series of "cyber war games" to prepare their government agencies for the potential of broad-based cyber-attacks on critical infrastructure, including the banking and financial sector (*BBC News*, 2015). War has both defensive and offensive aspects, both in real space and in cyber war. U.S. agencies define offensive cyber operations as activities intended "to manipulate, disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves," according to the Offensive Cyber Effects Operations (OCEO) presidential directive in 2012. The government employs several hackers to carry out offensive actions against cyber adversaries internationally. Too much emphasis is placed on

URI: https://hdl.handle.net/10125/63963
978-0-9981331-3-3

offensive retaliation by these hackers. Over-concentrating on offense can be dangerous and destabilizing because it encourages offensive actors to attack first and ferociously before an adversary can [34].

The term hacking has evolved over the years, but in general, it refers to the use of a computer to gain unauthorized access to information systems or to exploit the weaknesses of computer networks [21]. "Hacker" can mean either someone who compromises computer security or a skilled developer in the free or open-source software movements [22]. Hacks are deployed for various reasons as diverse as the thrill of the conquest, protests, profit, and bolstering status within the hacker community. Notably, hackers are not inherently bad, nor does the word "hacker" definitively mean "criminal."

Offensive security engineers are known as "red hat" hackers, who use hacking techniques to perform their job functions. (This is as opposed to "white-hat" hackers, who work primarily defensively, and "black-hat" hackers, who act maliciously). Red hats are considered the vigilantes of the hacker community when responding to cyber attribution. For several years, the U.S. military has employed offensive security engineers to attack cyber adversaries using potent cyber weapons or cyber tools that can break into enemy computers [18]. Offensive security techniques have since spread to business communities and social media platforms such as Facebook. Demand continues to grow in government and industry circles for engineers with offensive skills and ever-more-sophisticated cyber tools, including malicious software with such destructive potential as to qualify as cyberweapons implanted in an enemy's network [18].

Despite all of the security countermeasures implemented by security practitioners, the protection of data and other asset security is an ongoing process with no winners. As their work continues to evolve, offensive security engineers must know and adhere to the ethical practices of an organization so that the appropriate security policies are upheld, preventing illegitimate access. Yet, at the same time, they may easily succumb to their hacker vices when presented with an adversarial attack situation. This article investigates the ethical dichotomy of offensive security engineers, employing virtue (ethics) theory and cyber attribution. Therefore, answers were sought to the following specific research question:

Do offensive security engineers or hackers find it unethical to retaliate against nation-state actors?

2. Contribution to Information Systems

Modern threats — such as worms, viruses, phishing, denial-of-service (DoS) attacks, and botnets — underscore the need for offensive security research in an increasingly networked and computer-reliant society. Responses to these cyber threats vary from passive observation to the legal right to defend computer systems using aggressive countermeasures [14]. Such Internet security research is itself at one extreme of a broad spectrum of computer security research. We propose, however, that the information systems (IS) field should incorporate features of offensive security research which will require organizations to enable continued growth of the field.

3. Offensive Security Background

Currently, there are different authorities and rules of engagement for offensive as opposed to defensive cyber security. 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.

A major revelation of offensive security practices came with the discovery of Stuxnet in 2010, a computer sabotage operation reportedly conducted by the United States and Israel to destroy machines used in Iran's nuclear program. Stuxnet is a large, complex piece of malware with many different components and functionalities, written to target an industrial control system (ICS) or set of similar systems [15], such as those used in gas pipelines and power plants. Stuxnet is estimated to have infected 50,000 to 100,000 computers, mostly in Iran, India, Indonesia, and Pakistan [6] — unstable areas prior to possible cyber-prompted disruptions.

Moreover, U.S. intelligence agencies initiated 231 offensive cyber operations in 2011, nearly three-quarters of them against key targets such as Iran, Russia, China, and North Korea, some intended to disrupt nuclear proliferation [17]. This included placing covert implants in more than 80,000 machines around the world. And they are not alone; China and Russia are regarded as the most challenging cyber threats to the United States. U.S. intelligence has come to believe that China's state-employed hackers by day

return to work at night for personal profit, stealing valuable U.S. defense industry secrets and selling them [17] — so, threats are clearly present and must be addressed.

President Obama's directive on cyber-operations stated that military cyber-operations resulting in the disruption, destruction, or manipulation of computers must be approved by the president [38]. This specific directive is known as Presidential Policy Directive-20, or PPD-20, focuses on cybersecurity as a top priority. The policy considers the evolution of cyber threats to the growing U.S. infrastructure, establishing principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools. Relevant portions of PPD-20 include a restriction in type:

"Operations and related programs or activities — other than network defense, cyber collection, or DCEO — conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks."

They also offer some sense of the emergent nature of cyberthreats:

"Offensive Cyber Effects Operations OCEO can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging. The development and sustainment of OCEO capabilities, however, may require considerable time and effort if access and tools for a specific target do not already exist."

They further offer something of a mission statement:

"The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive."

Political science literature argues that military entities — such as those addressed by PPD-20 — are more prone to favor offensive operations than other kinds of bureaucracies [50]. Early evidence suggests that this "cult of the offensive" operates regarding cyber warfare. For example, James Cartwright, the former Vice Chairman of the U.S. Joint Chiefs of Staff, called for the United States to engage in more offensive cyber operations, and reportedly created a bureaucracy to that end [44]. And while government agencies, such as the U.S. National Security Agency (NSA), Department of Homeland Security (DHS), and the Defense Department's Cyber Command are responsible for defending government networks using offensive techniques, private companies are largely left to defend themselves on their own. In the wake of enormous cyberattacks on such companies as Uber, Equifax, Yahoo, and Sony, and the theft of e-mails from the DNC's server, some members of Congress are trying to pass a significant revision of the Computer Fraud and Abuse Act [41].

The bipartisan bill, known as the Active Cyber Defense Certainty Act (ACDCA), gives individuals and companies the legal authority to take action on networks, servers, and other infrastructures they do not own to establish attribution of an attack, disrupt an ongoing attack, and monitor the attacker. The bill proposes "to provide a defense to prosecution for fraud and related activity in connection with computers for persons defending against unauthorized intrusions into their computers." The majority of hacking incidents involve groups or nation-states that attack from servers outside of the United States — and outside the jurisdiction of the ACDCA legislation. Ultimately, the ACDCA wants to enable broader active cyber defense abilities to the private sector. Government legislation could make similar instances of collateral damage more common.

Some experts acknowledged that many companies already are pursuing attackers in ways that could be considered violations of the Computer Fraud and Abuse Act of 1986. The Computer Fraud and Abuse Act of 1986 prohibits anyone from "knowingly" accessing a computer "without authorization." The changes would permit companies, and private citizens, that are victims of cybercrimes to "hack-back," also referred to as active-defense [20]. It is essential for our society to be prepared and for businesses and governments to be ahead of the attackers and other actors with malicious intents. But this presents difficulties.

4. Offensive Cyber Attribution

Law enforcement and military authorities seeking to check malicious cyber activity face a fundamental challenge: the "attribution problem" [43]. This entails the task of identifying the author of a cyber-attack or cyber-exploitation. The attribution problem permeates the cybersecurity literature. Rid & Buchanan [39] noted that "the attribution debate is evolving surprisingly slowly," with an excessive focus on

technical forensics. They argued that attribution is not impossible for the defender, because even the most sophisticated attackers ultimately make mistakes, but it is difficult and resource-intensive, requiring specialized skills and substantial time invested. Moreover, a clever adversary can mask its tracks by routing attacks or exploitations through anonymizing computers around the globe.

Attributing a cyber operation through common techniques such as technical forensics, as well as other intelligence sources and situational context [3], reverse-engineering [7], source tracking [29], honeypots [48], and sink-holing [4] can prove difficult. Sometimes traceback and related forensic tools can provide adequate attribution. Human and other forms of intelligence-gathering can further aid in cyber attribution. The difficulty of this problem stems not only from the amount of effort required to find forensic clues, but also the ease with which an attacker can embed false clues to mislead security professionals [43]. Without sufficient attribution, it is not possible to enforce policy, law, or pacts to support business and government objectives. The inability to enforce laws makes creating new ones meaningless and gives malicious attackers little motivation to behave. Additionally, distinguishing between state-sponsored and private attacks has been under debate for years, making criteria for state responsibility unsettled. There are growing calls to deal with the cyber-attribution problem by making a nation responsible for all cyber-attacks that emerge from within its borders, even if the attacks are not sponsored by that nation [8]. Such calls increase the impetus to gain control of the online environment and on those who will act badly within it.

Foreign intelligence organizations are constantly trying to break into the networks that undergird U.S. military operations. Amid all this, military organizations have noted the success of cyber attackers in damaging computer systems and have hoped to use these same techniques or "exploits" for military advantage, much as they seek a wide variety of ways to gain advantage in warfare [11]. This is accomplished by employing offensive security engineers in the fight against cyber attribution using offensive techniques. The United States promotes its cyber warriors as the best at offense, with the capability of using cyberweapons against their adversaries [9], cyberweapons that can be launched or controlled either externally, from another computer or the Internet, or internally, by spies and saboteurs [25]. The goal of using cyberweapons is to take control of a system without the knowledge of the system's owner so it can be used for the offensive engineer's purposes, called "rootkits" [26]. Sets of such remotely controlled computers can be used to create "botnets," networks of computers gathered under the control of a single user [1]. Hacker botnets have been used for monetary gain by sending spam or phishing email from the slave computers, denial-of-service (DoS) attacks against organizations, sending ransomware to blackmail organizations by threatening malicious mischief, and engaging in cyber-espionage. Botnets developed for military purposes could stop an adversary's military from communicating or fully deploying its weapon systems, making their development attractive.

The DHS, NSA and Cyber Command's strategy for recruiting hackers relies, in part, on appeals to malice and mischievousness: at security conferences (e.g., Black Hat, DEFCON, B-Sides), agency representatives often pitch prospective applicants by promising work that might otherwise land them in prison. These recruiters often describe the job function as an "ethical hacker" or "white hat." Some security experts question whether the term "ethical hacker" is a contradiction in terms, as hacking was originally defined as a criminal activity and still carries that resonance. Conrad Constantine, a security research engineer at AlienVault, stated "The term 'ethical' is unnecessary – it is not logical to refer to a hacker as an 'ethical hacker' because they have moved over from the 'dark side' into 'the light'… The reason companies want to employ a hacker is not because they know the 'rules' to hacking, but because of the very fact that they do not play by the rules" (as cited in [2], p. 66). It is prudent to suspect that prior unprofessional hacking conduct eventually may overflow into official job duties. Few have mastered the rare art of maintaining multiple dispositions. Maintaining ethical standards for red-hat hackers, then, becomes an important concern.

5. Vice versus Virtue

Fieser [16] noted that, "The field of ethics (or moral philosophy) involves systematizing, defending, and recommending concepts of right and wrong behavior" [16]. Normative ethics is a subfield that seeks to develop a set of morals or guiding principles to influence the conduct of individuals and groups within a population (e.g., professional, religious, or societal). 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. Vice, then, is simply a deficiency or excess of virtue; virtue and vice are not exclusive or binary, but exist on continua

with one another, with virtue generally implying or even containing vice [30].

Some hackers who formerly engaged in thrill-seeking computer crimes are now assisting or employed by governments and companies to establish and maintain security practices by testing system vulnerability with their own specialized knowledge, thus helping to foil the activities of "black hat" malevolent cyber-attackers. This raises some ethical issues, particularly the question of whether such offensive hackers emphasize computer security as a professional virtue or whether they hack as a socially legitimatized vice. Hackers often discuss their motivations for hacking. These are sometimes characterized as self-justifications, as explanations, or as agonized struggles with personal obsessions and failures [24]. Additionally, hackers often confess to an addiction to computers or computer networks, a feeling that they are compelled to hack. The motivations offered by perhaps the most famous of all hackers, Kevin Mitnick, provides a common articulation of motivations for hacking [24]:

"You get a better understanding of cyberspace, the computer systems, the operating systems, how the computer systems interact with one another, that basically was my motivation behind my hacking activity in the past. It was just from the gain of knowledge and the thrill of adventure, nothing that was well and truly sinister as trying to get any type of monetary gain or anything."

In response to this dilemma, it could be argued that hackers have an ethic or ethos (Greek meaning custom, habit, character, or disposition) that is grounded in the ethical use of computers. There is evidence of such an ethic, which is not imposed by organizational codes of conduct [40], but is based on an intrinsic set of values and beliefs, inspired by an inherent respect for computers and the information they contain — and the cyber-attribution of those who do not share this respect. For example, some hackers have spent large amounts of their own time, for no apparent financial gain, in obsessively tracking down malicious cyber-attackers and bringing them to account for the damage they have caused, not only to organizations, but to the ethos of the former hacking community [45, 46]. But while the hacker ethic in response to cyber-attribution is one of exploration and retaliation without thought of virtue or consequences, tolerance of cyber-retaliation has changed over time, since threats and cyber harm have become more serious [28]. Thus, again, the ethical postures of those who would undertake offensive cybersecurity activities is a matter of concern for individuals, companies, and nations.

6. Methodology

A quantitative survey and descriptive statistics were adopted for this study. Data was collected through self-reporting using convenience sampling. This study focused primarily on offensive security engineers as the population being studied. Offensive security engineers are individuals that use hacking techniques to perform their jobs. Because the study was intended to reach a difficult demographic to survey, a "thank you" splash page at the end of the survey asked subjects to recommend friends to the survey, creating a self-perpetuating sample in accordance with the process of the snowball sampling technique.

In accordance with previously cited literature on hackers and computer security, the authors developed a survey instrument from the collection of preceding literature and articles. For the purpose of the survey design and data analysis, the authors organized questions that would be non-intrusive to the target population of offensive security engineers and hackers.

The research setting is non-contrived because participants used their computers or mobile devices to take the web-based survey. In addition to a web-based survey link, quick response (QR) codes were distributed electronically via LinkedIn groups and Twitter hacker communities.

A 12-item survey was developed and implemented using a Survey Monkey form. The survey included 10 questions that captured the perceptions of the "hack back" initiatives and ethical interpretations. Therefore, this survey seeks to gain feedback from offensive security engineers, red/black teams, or other hackers responsible for pursuing attackers as a key part of their job function.

Survey responses were analyzed using frequency analysis and Pearson's Chi-square ($p < .05$) and categorical analysis among demographic variables.

6.1 Participants

The final dataset for statistical analyses included 123 respondents. Of the 123 respondents, 115 (93.5%) were men and eight (6.5%) were women; the majority of the respondents were between the ages of 35 and 44 years (35.77%). Demographic statistics are displayed in Table 1.

Gender and age are often used in the reporting of demographic data; however, previous studies have varied in their use for examining statistical

differences. Researchers, Mensch and Wilkie [35] found differences in security attitude between men and women.

Table 1: Demographics (Age and Gender)

Age (in range)	Male	Female	Total	Percentage
18 - 24	5	0	5	4.1%
25 - 34	25	4	29	23.6%
35 - 44	40	4	44	35.8%
45 - 54	32	0	32	26.0%
55+	13	0	13	10.6%
Total	**115**	**8**	**123**	**100%**

Table 2: Survey Questions (Frequency and Category Analysis)

	Frequency Analysis					Category Analysis		
Survey Questions	**Strongly Agree**	**Agree**	**Neither Agree nor Disagree**	**Disagree**	**Strongly Disagree**	**Total**	**Gender**	**Age**
Q1. I am familiar with the industry terms "active cyber defense" or "hack back".	71 57.7%	37 30.1%	9 7.3%	5 4.1 %	1 0.8%	123 100%	***p*=.002**	*p*=.423 (NS)
Q2. A key part my job function is threat intelligence and to "hack back" any adversary who penetrates my network.	9 7.3%	21 17.1%	34 27.6%	33 26.8%	26 21.1%	123 100%	*p*=.486 (NS)	*p*=.182 (NS)
Q3. I find satisfaction in offensively mitigating attacks against my company's network.	33 26.8%	32 26.0%	35 28.5%	13 10.6%	10 8.1%	123 100%	***p*=.051 (NS)**	*p*=.963 (NS)
Q4. Private companies should be allowed to offensively pursue their attackers.	29 23.6%	33 26.8%	23 18.7%	19 15.4%	19 15.4%	123 100%	*p*=.268 (NS)	*p*=.370 (NS)
Q5. It is un-ethical to pursue attackers originating from foreign nation-states.	8 6.5%	14 11.4%	19 15.4%	39 31.7%	43 35.0%	123 100%	*p*=.478 (NS)	*p*=.802 (NS)
Q6. I am torn between company ethics and performing my offensive job functions against adversaries.	9 7.3%	24 19.5%	53 43.1%	24 19.5%	13 10.6%	123 100%	*p*=.252 (NS)	*p*=.461 (NS)
Q7. There should be no prosecution for fraud and related activity involving persons defending against unauthorized intrusions into their networks.	26 21.1%	30 24.4%	34 27.6%	21 17.1%	12 9.8%	123 100%	*p*=.220 (NS)	*p*=.814 (NS)
Q8. I prefer offensive security techniques rather than defensive techniques.	22 17.9%	19 15.4%	37 30.1%	31 25.2%	14 11.4%	123 100%	*p*=.487 (NS)	*p*=.141 (NS)
Q9. I enjoy hacking and creating new offensive security techniques to remain current against attacks.	35 28.5%	39 31.7%	28 22.8%	16 13.0%	5 4.1%	123 100%	*p*=.857 (NS)	*p*=.070 (NS)
Q10. I will protect my company network from attackers at any cost.	23 18.7%	26 21.1%	40 32.5%	23 18.7%	11 8.9%	123 100%	*p*=.258 (NS)	***p*=.016**

Note: When $p < .05$ at significance level, items are non-significant, as denoted with (NS).

7. Results

As shown in Table 1, more males than females participated in the survey. Research for this study and literature on hackers has not uncovered any significant evidence of female hackers [49]. This imbalance is disproportionate even in the field of computer-mediated technologies [47]. A number of factors explain the paucity of women generally in the computer sciences: childhood socialization, where boys are taught to relate to technology more easily than girls; education in computers occurs in a masculine environment; and a gender bias toward men in the language used in computer science [47, 49].

Table 2 presents the frequency and categorical analyses of survey responses by the respondents. The following discussion examines the frequency analysis for each table first followed by the categorical analysis.

7.1 Frequency Analysis

The survey contained 10 questions designed to assess how offensive security engineers or hackers report their own vices from a security perspective (Table 2). The questions were worded not to insinuate a hacker's vice. The available responses to these questions were in a "Strongly Agree to Strongly Disagree" 5-point Likert scale format.

Of the 123 respondents, 57.7% (strongly agree, n=71) and 30.1% (agree, n=37) had knowledge of the terms "active cyber defense" or "hack back." Also, 26.8% (strongly agree, n=33) and 26% (agree, n=32) said that they find satisfaction in offensively mitigating attacks, while 23.6% (strongly agree, n=29) and 26.8% (agree, n=33) self-reported that private companies should be allowed to "hack back" their adversaries. Additionally, 35% (strongly disagree, n=43) and 31.7% (disagree, n=39) self-reported that they do not find it unethical to pursue adversaries in foreign countries. Further, 21.1% (strongly agree, n=26) and 24.4% (agree, n=30) self-reported that there should be no prosecution for anyone who defends against foreign adversaries. In regard to motive, 28.5% (strongly agree, n=35) and 31.7% (agree, n=39) reported that they enjoy hacking and creating new offensive techniques or tools. Surprisingly, 43.1% (n=53) did not agree or disagree with whether they were torn between company ethics and performing offensive job functions.

When summing the responses for questions Q2 and Q10 respectively, 47.9% (n=59) of respondents reported that it is not part of their job function to "hack back" adversaries. On the other hand, 39.8% (n=49) reported that they would protect their network at all costs and 32.5% neither agreed nor disagreed.

7.2 Categorical Analysis

In addition to the descriptive measures reported above in Table 2, categorical analysis was done on demographic data in the study. The variables used were gender and age group. No predictions were made on these variables; the study was exploratory.

Table 2 contains Pearson's chi-squared statistics for each of the demographic variables. The only variable with more than one significant result was gender. Males responded more frequently (n=115) than females (n=8) and differently on all questions ($p<$ .05). Thus, we present the following analysis:

One significant difference was found for each of the age and gender variables. For age under Q10, "I will protect my company network from attackers at any cost," more respondents between the ages of 25 and 34 would protect their company network from foreign adversaries no matter the cost. The significant result was p=.016. On one hand, this may not be surprising — one might expect this age range to be quicker to attack their adversaries. Although the Pearson's chi-squared was p=.051 and not significant for Q3, it is still worthy to mention that more males find satisfaction in offensively protecting their company's network. Finally, for gender significance in Q1, "I am familiar with the industry terms 'active cyber defense' or 'hack back,' more males understood the terms (p=.002) presented in Q1. Among all respondents, only one female had never heard of the terms.

8. Conclusion

It is fair to conclude that the research question was answered. Based on the respondent's self-report, we found 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. Additionally, based on the frequency analysis, there appears to exist a dichotomy of vice versus virtue among offensive security engineers. A few of the questions elicited a high percentage of undecided (neither agree nor disagree) responses; this alludes to such a dichotomy.

As cybercrime continues to be an increasing and evolving threat, attention must turn toward long-term solutions. Simply blocking these attacks does not do so, but instead allows cybercriminals to improve their attacks, which is relatively easy to do in the current environment. Attribution is one of the most promising

ways to increase the risks associated with performing cybercrime, and therefore provide a way to reduce the frequency of cybercrime.

Most public discussion has centered on defense against cyberattacks on governmental, military, and economic concerns. Cyber activities can have defensive or offensive purposes. Defensive cyber activities include upgrading or restoring a computer system that has been damaged, investigating damage in the computer system, and maintaining situational awareness of computer systems and networks. Offensive cyber activities are the insertion of computer programs into an attacker's computer system to observe and collect transmitted information; the disruption, degradation, or destruction of the software of a system; the destruction of the hardware of a system; and the manipulation of a computer system to use it to cause further damage [42].

The hiring point for the government and most businesses is that hackers have considerable skillsets and knowledge about telecommunications, data security, operating systems, programming languages, networks, and cryptography as opposed to less skilled security professionals. Hackers are being employed to perform such offensive cyber activities. The offensive or red-hat hackers who have developed their unique skills by breaking into company and government systems are now being employed for purposes of offensive security against their former colleagues. The hacker ethos for securing computer systems is soon overshadowed by the vice of hacking for the thrill of it. The "attribution problem" will have consequences, requiring offensive hackers to identify and retaliate against attackers on domestic and foreign soil, rejecting state toleration of such cyber-adversaries.

In today's ever-evolving cyber threat landscape where cyber attackers are constantly searching for new ways to circumvent existing security and legislative controls to commit cybercriminal activities, it is essential for offensive hackers to possess current knowledge, skills, and experiences. It is unrealistic to expect that government agencies have all the cyber security expertise required in securing the nation's critical infrastructures. Therefore the "hack-back" initiative is slowly gaining momentum to legalize cyber-retaliation methods among businesses, currently prohibited by the Computer Fraud and Abuse Act.

9. Future Research

The paper as a whole is more interested in laying out the problem and its scope than in actually addressing the problem. Context is essential, to be sure, but the argument can be made that the possibility of vice overwhelming virtue among red-hat hackers and the ongoing concerns with cyber attribution present significant risks for the conduct of offensive cybersecurity activities, and that this issue needs to be given more attention (and space) than it currently receives.

The main limitations to this research are: (1) offensive hacker perceptions were measured as opposed to their actual behavior, and (2) the generalizability of the study is limited because the target participants only included offensive security engineers and hackers from a small population. The sample was unselected and is unlikely to contain many high-rate hackers. Future research might be usefully conducted in other hacker communities or conferences (i.e. Black Hat or DEFCON).

Therefore, one goal of future research would be to demonstrate through more behavioral evidence/attestation whether or not vice does overwhelm. Future investigations should consider developing a survey instrument, based on prior research, to measure the virtues and vices of offensive security professionals. The research would also possibly address philosophical systems that argue that vice inevitably wins out; these philosophies may provide a useful perspective on the general issue. Given that many hackers perceive themselves as libertarian or even Randian, those ideologies also may need to be investigated as a starting point for this work.

Further discussions in the information security field should be about the issue of trust. Some security professionals are opposed to hiring hackers for security work. Dr. Eugene Spafford of Purdue University is quoted as saying, "Do not do business with any company that hires a convicted hacker to work in the security area. …This is like having a known arsonist install a fire alarm." Those entities that do hire hackers overlook their potential for engaging in vice and hire them based on an extensive background check and assumption that they will perform their job functions and not violate the organization's trust or the trust of their clients. Most hired hackers do not misuse their power as they know they are being trusted with something important, and they want to live up to that trust. There are differing beliefs throughout the information technology community that favor both sides of the discussion. However, the importance of cybersecurity differs based on the differing focuses of the individual organizations. This also could be a topic of future research.

To stay ahead of its adversaries, the United States must constantly adjust and improve its cyber offenses and defenses. The U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit critical infrastructure's weaknesses.

Classifications of critical infrastructures vary across countries, but are united by the thought that the relevant asset must be "vital" to count as critical. DHS states that, "Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." It is unclear whether additional vulnerabilities are introduced to the critical infrastructure by performing offensive techniques or whether this is an underlying concern of the government. Further research may dive deeper into this question.

To date it has proven difficult to define clear rules of engagement for responding to cyberattacks. These rules of engagement will first have to assist in distinguishing among the exploits of a mere hacker, criminal activity (such as fraud or theft), espionage, or an attack by a foreign government entity [31]. The rules will need to describe or at least suggest what is necessary, appropriate, relative, and justified in each particular case, based on relevant domestic and international laws. Therefore, policy structures and ethics of offensive security techniques would be worth examining in future research.

10. References

[1] Bailey, Michael, Evan Cooke, Farnam Jahanian, Yunjing Xu, and Manish Karir. "A survey of botnet technology and defenses." In 2009 Cybersecurity Applications & Technology Conference for Homeland Security, pp. 299-304. IEEE, 2009.

[2] Bodhani, Aasha. "Bad... in a good way [Information Technology Security]." Engineering & Technology 7, no. 12 (2013): 64-68.

[3] Boebert, W. Earl. "A survey of challenges in attribution." In Proceedings of a workshop on Deterring CyberAttacks, pp. 41-54. 2010.

[4] Bradbury, Danny. "Fighting botnets with sinkholes." Network Security 2012, no. 8 (2012): 12-15.

[5] Chaubey, R. K. An Introduction to Cyber Crime and Cyber Law. Kamal Law House, 2009.

[6] Chen, Thomas M. "Stuxnet, the real start of cyber warfare?[Editor's Note]." IEEE Network 24, no. 6 (2010): 2-3.

[7] Chikofsky, Elliot J., and James H. Cross. "Reverse engineering and design recovery: A taxonomy." IEEE software 7, no. 1 (1990): 13-17.

[8] Clarke, Richard Alan, and Robert K. Knake. Cyber war. Tantor Media, Incorporated, 2014.

[9] Clarke, Richard. "War from cyberspace." The National Interest 104 (2009): 31-36.

[10] Cybint. 12 Alarming cyber security facts and stats. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/ ; (2018).

[11] Denning, Dorothy E. Information warfare and security. Reading, MA: Addison-Wesley; (1999) September.

[12] Kahn, Robert E., Mike McConnell, Joseph S. Nye Jr, Peter Schwartz, Nova J. Daly, Nathaniel Fick, Martha Finnemore et al. "America's cyber future." Center for A New American Security (2011).

[13] Dittrich, David, Michael Bailey, and Sven Dietrich. "Towards community standards for ethical behavior in computer security research." Technical Report (2009).

[14] Dittrich, David, and Kenneth E. Himma. "Active response to computer intrusions." The Handbook of Information Security 3 (2005).

[15] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5, no. 6 (2011): 29.

[16] Fieser, J. Ethics. Internet Encyclopedia of Philosophy. (2003).

[17] Gellman, Barton, and Ellen Nakashima. "US spy agencies mounted 231 offensive cyber-operations in 2011, documents show." The Washington Post 30 (2013).

[18] Gjelten, Tom. "First strike: US cyber warriors seize the offensive." World Affairs (2013): 33-43.

[19] Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony hack: Exporting instability through cyberspace." (2015).

[20] Himma, Kenneth Einar. Internet security: Hacking, counterhacking, and society. Jones & Bartlett Learning, 2007.

[21] Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. Cybercrime and digital forensics: An introduction. Routledge, 2017.

[22] Hoffman, Chris. "Hacker Hat Colors Explained: Black Hats, White Hats, and Gray Hats." How-To Geek. April 20 (2013).

[23] Inkster, Nigel. "Information warfare and the US presidential election." Survival 58, no. 5 (2016): 23-32.

[24] Jordan, Tim, and Paul Taylor. "A sociology of hackers." The Sociological Review 46, no. 4 (1998): 757-780.

[25] Knapp, Kenneth J., and William R. Boulton. "Ten information warfare trends." In Cyber Warfare and Cyber Terrorism, pp. 17-25. IGI Global, 2007.

[26] Kühnhauser, Winfried E. "Root Kits: an operating systems viewpoint." ACM SIGOPS Operating Systems Review 38, no. 1 (2004): 12-23.

[27] Lewis, James A. "The role of offensive cyber operations in NATO's collective defense." Tallinn Paper 9 (2015).

[28] Libicki, Martin C. Cyberdeterrence and cyberwar. Rand Corporation, 2009.

[29] Lipson, Howard F. *Tracking and tracing cyber-attacks: Technical challenges and global policy issues* (No. CMU/SEI-2002-SR-009). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST. (2002).

[30] Loftus, M. When virtue becomes vice. [Online]. Retrieved from: https://www.psychologytoday.com/us/articles/201309/when-virtue-becomes-vice ; 2013.

[31] Lynn III, William F. "Defending a new domain-the Pentagon's cyberstrategy." Foreign Affairs. 89 (2010): 97.

[32] Hoglund, Greg, and Gary McGraw. Exploiting software: How to break code. Pearson Education India, 2004.

[33] McGraw, Gary. Software security: building security in. Vol. 1. Addison-Wesley Professional, 2006..

[34] McGraw, Gary. "Cyber war is inevitable (unless we build security in)." Journal of Strategic Studies 36, no. 1 (2013): 109-119.

[35] Mensch, Scott, and L. Wilkie. "Information security activities of college students: An exploratory study." Academy of Information and Management Sciences Journal 14, no. 2 (2011): 91-116.

[36] Morgan, Steve. "Top 5 cybersecurity facts, figures and statistics for 2017." CSO Online (2018).

[37] Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia after the 2007 cyber attacks: Legal, strategic and organizational changes in cyber security." International Journal of Cyber Warfare and Terrorism (IJCWT) 1, no. 1 (2011): 24-34.

[38] Presidential Policy Directive – PPD-20. U.S. Cyber Operations Policy. [Online]. Retrieved from: https://fas.org/irp/offdocs/ppd/ppd-20.pdf ; (2012).

[39] Rid, Thomas, and Ben Buchanan. "Attributing cyber attacks." Journal of Strategic Studies 38, no. 1-2 (2015): 4-37.

[40] Roberts, Paula, and Jenny Webber. "Virtuous Hackers: developing ethical sensitivity in a community of practice." Australasian Journal of Information Systems 9, no. 2 (2002).

[41] Schmidle, Nicholas. The digital vigilantes who hack back. The New Yorker. [Online] Retrieved from: https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back; (2018).

[42] Schmitt, Michael N. "Cyber activities and the law of countermeasures." Peacetime Regime for State Activities in Cyberspace 3 (2013): 659-688.

[43] Shakarian, Paulo, Gerardo I. Simari, Geoffrey Moores, and Simon Parsons. "Cyber attribution: An argumentation-based approach." In Cyber Warfare, pp. 151-171. Springer, Cham, 2015.

[44] Shalal-Esa, Andrea. "Ex-US general urges frank talk on cyber weapons." Reuters, November 6 (2011).

[45] Shimomura, Tsutomu, and John Markoff. Take Down: The Pursuit and Capture of Kevin Mitnick, America's Most Notorious Cyber-criminal; by the Man who Did it. Secker & Warburg, 1996.

[46] Stoll, C. "The Cuckoo's Egg. New York City." (1989).

[47] Spertus, Ellen. "Why are there so few female computer scientists?." Cambridge, MA: MIT Artificial Intelligence Laboratory. (1991).

[48] Spitzner, Lance. Honeypots: tracking hackers. Vol. 1. Reading: Addison-Wesley, 2003.

[49] Turkle, Sherry. The second self: Computers and the human spirit. Mit Press, 2005.

[50] Van Evera, Stephen. "The cult of the offensive and the origins of the First World War." International security 9, no. 1 (1984): 58-107.