The Amorphous Nature of Hackers: An Exploratory Study

Kento Yasuhara
University of New Haven

Daniel Walnycky
University of New Haven

Ibrahim Baggili
University of New Haven

Ahmed Alhishwan
University of New Haven

THE AMORPHOUS NATURE OF HACKERS: AN EXPLORATORY STUDY

Kento Yasuhara[1], Daniel Walnycky[2], Ibrahim Baggili[2], Ahmed Alhishwan[2]

[1]Department of Psychology
College of Arts and Sciences
University of New Haven
KYasuhara@newhaven.edu

[2]Connecticute Institue of Technology
Cyber Forensics Research & Education Group (UNHcFREG)
Tagliatela College of Engineering, ECECS
University of New Haven, 300 Boston Post Rd, West Haven, CT 06516
{dwanlycky, ibaggili, aalhi1}@newhaven.edu

ABSTRACT

In this work, we aim to better understand outsider perspectives of the hacker community through a series of situation based survey questions. By doing this, we hope to gain insight into the overall reputation of hackers from participants in a wide range of technical and non-technical backgrounds. This is important to digital forensics since convicted hackers will be tried by people, each with their own perception of who hackers are. Do cyber crimes and national security issues negatively affect people's perceptions of hackers? Does hacktivism and information warfare positively affect people's perception of hackers? Do individual personality factors affect one's perception of hackers? To answer these questions in a systematic manner, we created two hypotheses. The first hypothesis tested participants' response in 9 scenarios whereas the second hypothesis tested the participants' response based on their scores on the Neuroticism-Extraversion-Openness Inventory (NEO) personality subscale. In brief, our results were indicative of how personality traits could influence perceptions of hackers and hacktivism. Possibilities for future research and implications for legal and criminal justice policy are discussed.

Keywords: Hacker perception survey, Hacker ideology, Hacker ethnography, Hacker culture, Hacker crimes, Cybercrimes, Hacktivists.

MOTIVATION

What you see and hear depends a good deal on where you are standing; it also depends on what sort of person you are. C.S. Lewis

Digital forensics deals with the Acquisition, Authentication, Analysis (AAA) and presentation of digital evidence. The presentation phase typically consists of evidence being presented in courts, where judges, lawyers, and juries become an imperative part of the legal decision making. This is especially important when prosecuting hackers. Much of the research in digital forensics has focused on the technical components of the domain, however, understanding the perception of hackers by people is understudied. Our work is important and timely as people are beginning to perceive hackers in a positive light, given their instrumental role in the release of important pieces of evidence that have improved the

security of government and private organizations. Given that judges, lawyers, and juries are people that have their own perceptions of hackers, it is critical that we gain a deeper understanding of how people perceive hackers in today's cyber economy.

1. INTRODUCTION

There has been steady growth in cybercrimes over the past five years. With the increased use of social media such as Facebook, Instagram, and Snapchat, as well as messaging applications such as WhatsApp and Viber, technology has improved and integrated with our ordinary lives, which has increased an individual's susceptibility to cybercrimes and hackers. Subsequently, prosecution of cybercriminals and hackers have increased as well as enactment of laws prohibiting the use of technology to harm others. As the awareness and victimization by hackers increase, it is vital to determine perceptions of hackers and how this could be influenced by internal and external factors.

Hackers have existed in popular culture for decades. Representations of hackers have been based mostly from an outsider perspective, although recently, there have been more accurate portrayals using insider knowledge. Movie directors, news reporters, and journalists have often showcased shallow surface level dissections of hacker ideology and subculture. As hacker presence in media has grown, so has our misunderstanding about them, what they do, and the reasons behind their actions (Taylor, 2012).

Our work highlights the common perceptions of hacking motives and the relationship between these perceptions and personality characteristics. This exploratory study highlights a need for research within the field of perception of cybercrimes as well as the perception of hackers. As the integration of technology into our daily life continues, it will be important for the criminal justice system to determine how lay individuals perceive hackers and cybercrimes, as they might serve on a jury in such cases. Such integration has had influences within the political realm, with the current controversies surrounding Russian hacking of social media outlets to influence voters in the 2016 U.S. Elections. Our work resulted in the following contributions:

- It explores the utility of a dichotomous answer hypothetical scenario to determine perception.
- It catalyzes hacker perception research by presenting future work and open ended problems.
- Our multidisciplinary work involves fields of forensic psychology, criminal justice, and computer science.
- To the best of our knowledge, this is the only study which asked about the perception of hackers involving the use of social media and the elections before the rise of questions regarding Russian influences in the 2016 U.S. elections.

The rest of the paper is organized as follows. In Section 2 we provided an overview of related work. Section 3 details the methodology used to test the hypotheses and explains how this study was conducted. In Section 4, we shared our quantitative and qualitative results. Section 5 discusses the results as well as the limitations of our study followed by Section 7 where we shed light on future work. We concluded our work in Section 8.

2. RELATED WORK

2.1 Hackers viewed from afar

In the following section we highlight how the public generally views hackers and their subculture from afar.

2.1.1 Perception by the media

A major source for our understanding of hackers comes from the media. Often, when hackers are mentioned in the media, negative connotations are attached to the news stories. When the media only paints hackers as criminals or elitists, it leaves little room for the mass population to see them in a different light. Stanley (2015) discussed how propaganda effectively exploits and strengthens flawed ideologies and "robs

individuals of knowledge of their own mental states by systematically concealing their interests from them". This described mass manipulation brought on by deep rooted fear within the population. Intended or unintended, fear mongering is a result of these negative news stories.

2.1.2 Negative activities

The term hacking or hackers is perceived to always be related to criminal activity. The phrase hacker has been used as a synonym for cybercriminal (Barber, 2001). Although society groups hackers as a homogeneous group, their activities and motives may vary. Some of the examples in which hackers are portrayed negatively include: the billion dollar industry of dark net black market trading publicized from the silk road bust (Greenberg, 2013), bank hacking and massive credit card theft in the Bank Muscat hacks (Hammersley, 2014), espionage attacks (Gallagher, 2014), software pirates (Kiss, 2013), corrupt regime surveillance software suppliers (Hern, 2015), and social engineering con artists (Roose, 2016). There also appears to be gender and race related activities, such as anti-feminism (Hess, 2014) and cyber hate crimes (Citron, 2014). There are other related hacker activities, such as celebrity nude distribution (Zdziarski, 2014), spying on one's every move (Shahani, 2015), releasing felons from jails (Gallagher, 2011), and forcing airplanes to land (Marsh, 2015).

Security vulnerabilities and malware are an ever growing challenge and near impossible to be completely prevented. From Java and Flash exploits to security bugs like Heartbleed and Shellshock, the security sector has needed to grow as threats have become detailed and complex causing a fear of cyber warfare coupled with the increase in the need for experts in cybersecurity (Perez & Prokupecz, 2015). Recently, A Computer Emergency Response Team (CERT) report detailed the largest known cyber attack to a power grid which was carried out by Russian hackers in December 2015 against three separate Ukrainian power plants, taking out power for nearly a quarter of a million people (Whittaker, 2016). While we continue to see cyber attacks, it is important to consider the psychological elements behind such behavior.

Past work explained motivations of cyber criminals to be money, emotion, sexual impulses, politics/religion, and "just for fun" (Chakravarthy, 2014). Saroha (2014) attempted to gain a better understanding of hackers through interviews in order to determine common themes and characteristics among cybercriminals. The study found that hackers were intelligent, driven, introverted, and tinkerers. Previous self-reported studies have indicated that those more likely to commit crimes were introverted and shy and usually lacked internalization of societal norm (Rogers, Seigfried, & Tidke, 2006). Studies have also indicated that many hackers also show signs of antisocial behaviors, autism, and/or depression. In a study of antisocial personality and hackers, Padhye and Gujar (2012) found that that "cyber criminals with Antisocial Personality Disorder (ASPD) were more likely to impersonate others".

Studies have found links between personality traits and deviant computer behavior. Rogers et al. (2006) conducted a study with self-reported surveys regarding computer criminal behavior. The results showed that being introverted was a strong indicator in determining computer deviant/criminal behavior. Furthermore, Padhye and Gujar (2012) determined that individuals with ASPD were more likely to impersonate others when conducting deviant behavior.

Such concerns have led researchers to explore screening tools to identify hackers (I. M. Baggili, 2009). I. Baggili and Rogers (2009) found that pre-employment integrity was more effective in finding cybercriminals than actual anonymity. Other work focused on profiling of cybercriminals and finding certain reoccurring characteristics that appear in cybercriminals to help businesses keep hackers out of their employee lists (Nykodym, Taylor, & Vilela, 2005) .

2.1.3 Positive activities

Although the negative impacts of hackers are often highlighted, they have also contributed in a positive manner to society. Hackers like L0pht have dedicated themselves to help individuals

as well as governments understand the security problems of the digital age and the consequences of ignoring the issue (Timberg, 2015). More recently, the Electronic Frontier Foundation (EFF) and rogue cyber journalists like Jacob Applebaum helped disseminate information regarding Internet privacy and security.

Other self-described hackers such as Jon Zdzarski have helped law enforcement catch criminals with tools he created based on iOS exploits he discovered. Specifically, hackers may have a positive societal impact in various ways. From civic hackers that make communities better, to privacy advocates who stand up for everyone's Internet freedom, to open source software creators that enable people to contribute and critique the work; in addition to, security testing of government and corporation systems to make data and people safer (Shaw, 2006).

Many hackers are believed to have a positive impact on society (Glenny, 2011). Others have noted the importance of having hackers, for their technology and business abilities. There are also discussions noting the need for governments to employ hackers to help combat cyber warfare (Bijou, 2015). There are examples, such as Anonymous' campaigns against various groups, such as the KKK, Mexican drug cartels, North Korea, and the Westboro Baptist Church, which could be viewed as illegal, but some may argue have had a positive ethical and moral impact.

2.1.4 Perception by Entertainment Media

The entertainment world often paints an inaccurate picture as well. Many movies, television shows, and video games treat hackers as social rejects looking to get revenge or create chaos to entertain themselves. There are many examples of this, such as crashing the New York stock exchange in the movie Hackers, gaining access to nuclear weapons in the movie War Games, tapping into electronic grids in the game Watchdogs. There are also portrayals of hackers as a hero, providing necessary hacks for the 'good guys.' When entertainment portrays hacking, it is construed as complicated and confusing for all, contributing to the fear of the unknown for hacking and hackers.

Throughout history, humans have created fictional allegories to represent non-fictional truths. Hackers have been noted by some as modern day wizards, as "any sufficiently advanced technology is indistinguishable from magic" (Clarke, 1973). Command line code and new technological machinery, to some, may be a modern representation of magical spells and items. This analogy can be furthered by viewing the six aspects of hacking culture, technology, secrecy, anonymity, membership fluidity, male dominance and motivations, which are similar to depictions of wizard covens (Jordan & Taylor, 1998).

2.2 Hackers viewed from within

Perception of hackers from the outside is skewed from reality, however, there is little known about the internal motivations to hacking and hackers. Prior work has been conducted by the Institute for Security and Open Methodologies (ISECOM) to attempt to profile hackers and understand their internal motivations (Chiesa, Ducci, & Ciappi, 2008). Research has indicated that hackers may have a need for higher cognitive tasks as well as have a tendency to pursue higher risk activities than normal (Bachmann, 2010). They also seem to have a rational thinking style which leads to enjoyment of critical and complex problems (Bachmann, 2010). Furthermore, Young, Zhang, and Prybutok (2007) found that hackers value the practical nature of hacking and believe that there is a lower likelihood of penalties given to such activities. Other work has explored research in Neuro-Linguistic Programming to turn talented but misguided Information Technology personnel away from a beckoning Black Hat career (Gold, 2014). These perceptions have led to Hacktivist organizations (e.g. Lulzsec) to beliefs that there may be morally acceptable hacking activities, even though they are criminally punishable. Such behavior has been seen with activities from organizations such as Anonymous, Lulzsec, and Wikileaks, which have been backed by the community as socially acceptable and morally correct (Benzinga, 2011).

2.3 Changes to Perception of Hackers

Kleinknecht (2003) interviewed hackers and determined the following ways to improve our perceptions of hackers to manage the stigma attached to their deviant public identity:

1. Condemning “inaccurate" media portrayals of their subculture.
2. Imputing labels to others within the subculture to differentiate between “good" and “bad" hackers.
3. Invoking the hacker ideology as a vocabulary of motive.
4. Linking their perspective to outsiders viewed favorably by the public.

Bracy (2013) noted a different perspective on hacking and hackers. She explained that the Wright brothers, Nikola Tesla, and Ben Franklin were all inventors, but also, in todays terms, hackers. Hacking can be defined as amateur innovations, problem solving, and reverse engineering within an existing system. Some hackers, as noted previously, have been seen as activists and patriots.

The reality of hacking is difficult to determine, as civic hackers have shown an ability for citizens to change governments and influence society. Akin to the human immune system, hackers can both be society’s defenses against the dangers of the information age as well as a weapon used against it (Elazari, 2014). Hacking has been helpful in the transfer of knowledge, improvement of technology, and safeguards against threats on digital freedom (Kumar, 2014; Walnycky, Baggili, Marrington, Moore, & Breitinger, 2015).

3. METHODOLOGY

We developed a questionnaire (See Appendix A and Section 3.3) and applied for Institutional Review Board (IRB) approval, which was granted. Our goal was to test for the following major hypotheses:

- Hypothesis 1: Participants would believe that hacking behavior is “bad" and will choose the “bad" option in all hypothetical scenarios.
- Hypothesis 2: Participant scores on the NEO subscales will have an influence on decision making regarding choosing the “good" or “bad" option.

3.1 Participants

Table 1: Survey Respondent Demographics.

Colleges	***Frequency***	***%***
College of Criminal Justice & Forensic Sciences	102	83.6
College of Art & Sciences	12	9.8
College of Engineering	1	.8
College of Business	6	4.9
Undecided/Undeclared	1	.8
Race	***Frequency***	***%***
White	102	83.6
Black or African American	12	9.8
American Indian or Alaska Native	1	.8
Asian	6	4.9
No Response	1	.8
Gender	***Frequency***	***%***
Male	54	44.3
Female	67	54.9
Other	1	.8
Age	***Frequency***	***%***
18	26	21.3
19	37	30.3
20	25	20.5
21	23	18.9
22	6	4.9
32	1	.8
34	1	.8

A total of ($n = 135$) university students attempted the survey, 122 were complete. Undergraduate students have been used in research regarding jury decision making and mock juries. Research in mock jury decision making has noted the appropriateness of using this population in initial tests of important issues (Bornstein, 1999; Wiener, Krauss, & Lieberman, 2011). The participants’ ages ranged from 18-34 ($M = 19.84, SD = 2.13$), gender distribution was 44% male and 56% female. Participants were enrolled in 18 various majors within the University, including those who indicated undecided,

however, participants majoring in Criminal Justice (50%) were most common. Racial breakdown of the participants was 83.6% Caucasian, 9.8% African-American, 4.9% Asian, 0.8% American Indian or Alaskan Native, and 0.8% No response. There was also a range of religions, 13 different religions were indicated, with the most common being Christian (23.8%), Catholic (41.8%), and No preference (16.4%). The demographic details are presented in Table 1.

3.2 Procedures

Eligible participants were recruited by e-mail solicitation or classroom visitation with the permission of the instructor. The e-mail solicitations included a link to the questionnaire and classroom visitations involved the gathering of e-mail addresses of those who were interested in participating. Quantitative data analysis was conducted using IBM SPSS Statistics Version 23.

3.3 Measures

All questionnaires were administered using a secure website. The survey gave a general definition of hackers and hacking, then asked nine hypothetical scenarios of hackers actions, such as "a hacker has hacked into the computer of a suspected pedophile for evidence to give to police". After each scenario, participants were given two reasons for the hacker's actions, one of which was "good" (such as providing justice or helping others) and the other was "bad" (such as causing problems for others or financial benefits to oneself). After answers were given for the scenarios, individuals were asked about their thoughts about hacking, hackers, hacking in the media, and social engineering. Finally, they were given a very brief measure of the Big-Five personality domains (Gosling, Rentfrow, & Swann, 2003), and asked for basic demographic information. All questions can be found in Appendix A.

4. RESULTS

4.1 Quantitative Results

A one-sample Chi-Square Test was conducted to determine if there was a significant difference between the choice of "good" or "bad" motivations for the hacker scenarios (hypothesis 1). A binary logistic regression was performed to ascertain the effects the personality factors had on the likelihood that participants would choose the "good" or "bad" motivation per question (hypothesis 2). There were significant differences in several scenarios. Our results are shared per question.

When respondents were asked regarding the reasons behind a hack related to the early release of a movie, participants chose between a socially good motivation (condemning the film and muzzling marketing efforts) or a socially "bad" or selfish motivation (release it free to the public early); 75% of participants chose the latter rather than the former motivation ($X^2(1, N = 122) = 31.51, p < .001$). The results indicated that participants believed hackers to be socially "bad" in this condition, believing that they would want to release it free to the public early rather than to muzzle marketing efforts. Contrary to hypothesis 2, there were no significant differences between Neuroticism-Extraversion-Openness (NEO) personality sub-scale scores between those who chose the "good" or "bad" option ($X^2(5) = 4.12, p = 0.53$).

When respondents were asked about the motives of hacking into a prison, participants chose between a social "good" motivation (hacker believes prisoners were wrongfully convicted) or a social "bad" or selfish motivation (wanted to see anarchy), 73% of participants chose the latter rather than the former motivation ($X^2(1, N = 122) = 27.57, p < .001$), indicating that, as per our hypothesis 1, participants believe hackers to be "bad". Contrary to hypothesis 2, there were no significant differences between NEO personality sub-scale scores between those who chose the "good" or "bad" option ($X^2(5) = 6.53, p = 0.26$).

On a question regarding the motivation regarding hacking into a pedophile's computer for information to give to law enforcement, 88.5% of participants chose the socially "good" motivation

(wanting justice) over the socially "bad" or selfish motivation (wanting to show the power of hacking) ($X^2(1, N = 122) = 69.38, p < .001$). The results indicated, contrary to hypothesis 1, that the participants believed the hacker to be provoked by the socially "good" motivation. When looking at differences between the "good" and "bad" motivations based on NEO personality sub-scale scores, the logistic regression model was statistically significant, ($X^2(5) = 11.27, p = .05$), providing evidence for hypothesis 2. The model explained 17.3% ($NagelkerkeR^2$) of the variance in the choice made. An increase in the emotional stability scale was associated with a higher likelihood of a participant selecting the "bad" motivation, whereas an increase in the openness scale was associated with a higher likelihood of a participant selecting the "good" motivation.

On a question regarding hacking of an ex-employee into the Chief Executive Officer (CEO) of his former company, there was no significant difference between the "good" (exposing the unethical actions of his previous employer) or "bad" motivation (getting revenge for being fired) ($X^2(1, N = 122) = .295, p = .587$). There were no significant differences within NEO personality sub-scale scores between those who chose the "good" or "bad" motivation. The results indicated that, contrary to hypothesis 1, participants were mixed in their beliefs about hackers. Additionally, contrary to hypothesis 2, there were no personality differences observed between participants who chose the "good" or "bad" motivation ($X^2(5) = .84, p = 0.96$).

On a question regarding hacking into a celebrities' cellphone to share nude photos of the celebrity on the Internet, there was a significant difference between the choices of motivations, as 80% of participants chose the "bad" (hacking out of sexual desire) rather than the "good" (hacking to show security flaws) ($X^2(1, N = 122) = 127.2, p < .001$). There were no significant differences between NEO personality subscale scores between those who chose the "good" or "bad" motivation. The results indicate that, per hypothesis 1, individuals believed hackers to be motivated by the socially "bad" motivation rather than the "good" motivation. Contrary to hypothesis 2, there were no personality differences observed between participants who chose the "good" or "bad" motivation ($X^2(5) = 4.77, p = 0.45$).

On a question regarding hacking of an ex romantic partner, there was a significant difference between the motivations, as 91% of participants chose the "bad" (wanting to see his former partner suffer) rather than the "good" (the new romantic partner being abusive and needing to take action) ($X^2(1, N = 122) = 183.5, p < .001$). The results indicated that, per hypothesis 1, individuals believed hackers to be motivated by the socially "bad" motivation rather than the "good." Additionally, per hypothesis 2, the logistic regression model was statistically significant, ($X^2(5) = 10.67, p = .05$), providing evidence for hypothesis 2. The model explained 18.5% ($NagelkerkeR^2$) of the variance in the choice made. An increase in the conscientiousness scale score was associated with a higher likelihood of a participant selecting the "bad" motivation.

On a question regarding hacking of a black market website that sells stolen credit cards, there was a significant difference between the choices, as 59.8% of participants chose the "good" motivation (preventing innocent people's credit card from being sold) rather than the "bad" (blackmail site owner into giving the hacker a portion of the profits) ($X^2(1, N = 122) = 4.7, p = .03$). There were no significant differences between NEO personality sub-scale scores between those who chose the "good" or "bad" motivation. Contrary to hypothesis 1, participants believed that hackers were motivated by a socially "good" rather than a "bad" reason. Additionally, contrary to hypothesis 2, there were no differences in personality scores for individuals who chose the "good" or "bad" motivation ($X^2(5) = 3.97, p = .55$).

On a question regarding the reasons why a hacker created a botnet, there was a significant difference between the choices, as 73.8% chose the "bad" motivation (hacking into company/government servers) rather than the "good" (mine bitcoins to give to charity) ($X^2(1, N = 122) = 27.5, p < .001$). The results indicated, per hypothesis 1, that participants believed hack-

ers to have a “bad" motivation rather than a “good" motivation. Additionally, contrary to hypothesis 2, there were no differences in personality scores for individuals who chose the “good" or “bad" option ($X^2(5) = 6.77, p = .24$).

Finally, on a question regarding the hacking of a presidential candidate's twitter account, there was no significant difference between the two motivations (spreading awareness of something the candidate did that was covered up vs. saying lewd and inappropriate things for fun on the account) ($X^2(1, N = 122) = 2.1, p = .15$). The results indicated that, contrary to hypothesis 1, participants did not agree on a motivation between the two motivations. Additionally, contrary to hypothesis 2, there were no significant differences between those who chose the “good" or “bad" motivation in terms of personality subscale scores between those who chose the “good" or “bad" option ($X^2(5) = 4.08, p = .54$).

4.2 Qualitative Results

Open ended questions were also asked regarding respondents' thoughts on hackers and hacking. Participants were asked what they believe hackers are motivated by. Although some participants noted multiple motivations (therefore the percentages do not add up to 100), the most noted motivations were in the following descending order:

- Personal gain (27.9%)
- Greed (23%)
- Injustice (21.3%)
- Power (18%)
- Revenge (17.2%)

Participants were also asked when hacking would be okay. The most popular responses were:

- Hacking in the service of safety and/or justice (29.5%)
- Hacking is never okay (23%)
- Hacking when used to apprehend criminals (22.1%)

When asked when is social engineering would be okay, the most popular responses were:

- It was never okay (41%)
- Use for safety and capturing/interrogating criminals (both at 18.9%)

Participants were also asked if hacktivists were extremists.

- 46% of respondents noted yes
- 22% noted no
- 23.8% noted that it would depend on the situation.

Finally, participants were asked what the penalty should be for someone who was caught for hacking. The most common responses were:

- Jail time (34.4%)
- Depending on the situation (32.7%)
- A fine (21.3%)
- Prison time (17.2%)
- Disallowing usage of computing devices (10.7%).

5. DISCUSSION

There were two aims to this study. One was to determine the general perception of hackers. The second was to determine if there was a link between personality traits (measured using the Big-Five) and perception of hackers.

By examining the general perception of hackers, contrary to hypothesis 1, there was no consistent pattern in how hackers were perceived (i.e. they were not consistently seen as “bad" or “good"). It was, however, interesting that in seven of nine scenarios, participants generally agreed regarding the motives behind the hacker. This could be due to two reasons. Although we conducted pilot testing and research to have vignettes that were reasonable, one reason for the difference could be the “bad" and “good" scenarios in the vignettes were unreasonable or unrealistic, which biased the answers. The other reason could be that there is a common perception of how hackers act in certain situations, not a common perception of hacker motives in general. Like all individuals, participants tended to view

hackers within a spectrum, that they were, as a group, both capable of “good" and “bad".

By examining the link between personality traits and perception of hackers, we found differing results for varying scenarios. We found differences in motivation choices when looking at the scenario related to hacking into a prison (for the emotional stability and openness scales) and hacking into an ex romantic partner (conscientiousness scale).

Although there were fewer significant differences in personality factors which influenced decision making than hypothesized, the differences which were found are of interest. When looking specifically at the hacking in prison scenario, individuals who were higher on the openness scale were more likely to believe that hacking was due to freeing prisoners based on wrongful convictions. Individuals who are high on openness are more likely to desire novel experiences, self-reflect, and have the ability to make new connections between seemingly contradictory ideas. Such individuals may have been able to make an easier connection between the "good" motivation (freeing prisoners who should not be in prison) with a contradictory idea, conducting criminal behavior (hacking).

Finally when we looked at the ex romantic partner scenario, individuals who were higher on the conscientiousness scale were more likely to believe that the hacking was due to wanting to see a former partner suffer. Individuals that score high on the conscientiousness scale tend to control impulses and act in a socially acceptable way, as well as facilitate goal-directed behavior. Such individuals tend to be able to delay gratification and plan as well as organize effectively. Considering such traits, this result is surprising. The results could be due to such individuals believing that hacking is a socially acceptable way to retaliate and may have believed that the suffering of the former partner was somehow deserved.

6. LIMITATIONS

There were several limitations to this work. The first was the survey methodology. Although this was a novel and effective means of forcing individuals to make choices between “good" and “bad", the choices themselves could have been problematic or unrealistic for participants. Although a pilot survey revealed a consensus regarding “good" and “bad" scenarios, individuals may interpret the “good" and “bad" scenarios in an alternate manner. Additionally, the age range of participants was limited, therefore, there could be issues with generalizability to a larger population, especially when this generation may have a different perception of hackers and cybercriminals. Further, these were all college students, which would also create issues in generalizability. Lastly, we had a larger quantity of individuals who had academic knowledge within the criminal justice field, which may, as a field, have a common perception of hacker motivations in different scenarios.

7. FUTURE WORK

As noted previously, this is one of the first studies examining the perception of hackers as well as personality traits and its relation to such perceptions. As technological advances continue to automate much of our lives, hackers will gain more opportunities to become influential in the lives of lay individuals. As such, perception of hackers will become important, especially when considering policy and criminal justice implications into punishment and rehabilitation of hackers and hacking organizations. There are several realms that can be noted for future work. One study could examine testing across situations and across professions.

To our knowledge, there is little research on how perception of hackers may differ from the perception of other professions, such as law enforcement, medical professionals, or general contractors. There has been, especially within law enforcement, research on public perception of use of force and specific aspects of the law enforcement profession. A comparison between legitimate professions vs. hackers may be informative, as it could reveal differences or similarities between perceptions of other professions.

Additionally, future research should concentrate on a broader sample with a broader age

range of individuals, as perception of hackers could vary by age. For example, there may be other moderating factors, such as cybercriminal engagement (I. M. Baggili, 2009; I. Baggili & Rogers, 2009).

A longitudinal study exploring changes in perception of hackers would improve the generalizablity of results. As time passes, society will be come more technologically integrated, therefore, issues with hackers may become more personal and visible. There have been studies that have attempted to manipulate people's perception of technological use (I. Baggili, Al Shamlan, Al Jabri, & Al Zaabi, 2012). Similarly, an experiment manipulating one's perceptions of hackers would be informative. As noted, the criminal justice system is likely to have more cases related to hackers and manipulation of hackers could influence jury decision making. For example, would it make a difference for people to use the word "hacker" vs. "cybercriminal" in people's perception of hacker motivations

Finally, specifically related to our last hypothetical regarding a presidential candidate's twitter account, it would be interesting to conduct this question again as it would be assumed that people's perceptions of hackers may have changed, specifically with regard to this question, considering the current political climate and issues surrounding the hacker's influence on the U.S. presidential election.

8. CONCLUSION

This study found some initial differences in perception of hackers and some relationships between personality factors and perception of hackers. Such findings have practical utility within the criminal justice system. The criminal justice system, specifically juries, have innate biases towards different types of offenders, however, there have been no previous studies on the biases towards hackers. Such information would be useful for both defense and prosecution attorneys as well as judges when involved in cases of hacking or the use of hackers.

Additionally, this information could be useful in cybercriminal profiling, where innate and personal biases may skew one's ability to have an accurate profile. Finally, this research can assist in law enforcement's ability to discuss and formulate effective plans against hackers. If we are able to determine factors which influence individuals' perception of hackers, such factors can be incorporated into training for law enforcement, specifically those who work with or may have heavy involvement within the cybercriminal realm. This would increase the ability for law enforcement to have constructive and effective strategies in combating hackers.

REFERENCES

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology*, *4*(1/2), 643.

Baggili, I., Al Shamlan, M., Al Jabri, B., & Al Zaabi, A. (2012). Cybercrime, censorship, perception and bypassing controls: An exploratory study. In *International conference on digital forensics and cyber crime* (pp. 91–108).

Baggili, I., & Rogers, M. (2009). Self-reported cyber crime: An analysis on the effects of anonymity and pre-employment integrity. *International Journal of Cyber Criminology*, *3*(2). Retrieved from http://www.cybercrimejournal.com/ibrahimmarcusIJCCJuly2009.pdf

Baggili, I. M. (2009). *Effects of anonymity, pre-employment integrity and antisocial behavior on self-reported cyber crime engagement: An exploratory study* (Unpublished doctoral dissertation). Purdue University.

Barber, R. (2001). Hackers profiled — who are they and what are their motivations? *Computer Fraud and Security*, *2001*(2), 14 - 17. Retrieved from http://www.sciencedirect.com/science/article/pii/S1361372301020176 doi: http://dx.doi.org/10.1016/S1361-3723(01)02017-6

Benzinga, J. (2011). Lulzsec, anonymous are freedom fighters. *Business Insider*. Retrieved from

http://www.businessinsider.com/lulzsec-anonymous-are-freedom-fighters-2011-6

Bijou, R. (2015). Governments don't understand cyber warfare. we need hackers.

Bornstein, B. H. (1999). The ecological validity of jury simulations: Is the jury still out? *Law and human Behavior*, *23*(1), 75–91.

Bracy, C. (2013). Why good hackers make good citizens.

Chakravarthy, A. (2014). Analysis of cyber-criminal profiling and cyber-attacks: A comprehensive study. *World Conference on Applied Sciences*.

Chiesa, R., Ducci, S., & Ciappi, S. (2008). *Profiling hackers: the science of criminal profiling as applied to the world of hacking* (Vol. 49). CRC Press.

Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.

Clarke, A. (1973). Clarke's three laws.

Elazari, K. (2014). Hackers: the internet's immune system.

Gallagher, S. (2011). Vulnerabilities give hackers ability to open prison cells from afar. *arstechnica*.

Gallagher, S. (2014). "epic" fail—how opm hackers tapped the mother lode of espionage data. *arstechnica*.

Glenny, M. (2011). Hire the hackers!

Gold, S. (2014, Feb). Get your head around hacker psychology [information technology cyber-security]. *Engineering Technology*, *9*(1), 76-80. doi: 10.1049/et.2014.0111

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the big-five personality domains. *Journal of Research in personality*, *37*(6), 504–528.

Greenberg, A. (2013). End of the silk road: Fbi says it's busted the web's biggest anonymous drug black market.

Hammersley, B. (2014). Cyber-heists: Organised crime's credit card theft rampage. *BBC News*. Retrieved from http://www.bbc.com/news/technology-29937536

Hern, A. (2015). Hacking team hack casts spotlight on murky world of state surveillance. *theguardian*. Retrieved from http://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights

Hess, A. (2014). Why women aren't welcome on the internet. *Pacific Standard*, *6*.

Jordan, T., & Taylor, P. (1998). A sociology of hackers.

Kiss, J. (2013). The pirate bay trial: guilty verdict. Retrieved from http://www.theguardian.com/technology/2009/apr/17/the-pirate-bay-trial-guilty-verdict

Kleinknecht, S. (2003). *Hacking hackers: Ethnographic insights into the hacking subculture – definition, ideology, and argot.* Retrieved from https://macsphere.mcmaster.ca/bitstream/11375/10956/1/fulltext.pdf

Kumar, M. (2014). Project zero - a team of star-hackers hired by google to protect the internet. *The Hacker News*. Retrieved from https://thehackernews.com/2014/07/project-zero-team-of-star-hackers-hired

Marsh, R. (2015). Hackers successfully ground 1,400 passengers. *CNN*. Retrieved from http://www.cnn.com/2015/06/22/politics/lot-polish-airlines-hackers-ground-planes/

Nykodym, N., Taylor, R., & Vilela, J. (2005, December). Criminal profiling and insider cyber crime. *Digit. Investig.*, *2*(4), 261–267. Retrieved from http://dx.doi.org/10.1016/j.diin.2005.11.004 doi: 10.1016/j.diin.2005.11.004

Padhye, V., & Gujar, M. (2012). Virtual impersonation by antisocial personalities in cybercrime. *International Journal of Science*, *1*(2).

Perez, E., & Prokupecz, S. (2015). First on cnn: Newly discovered hack has u.s. fearing foreign infiltration. *CNN*. Retrieved from http://www.cnn.com/2015/12/18/politics/juniper-networks-us-government-security-hack/

Rogers, M. K., Seigfried, K., & Tidke, K. (2006, September). Self-reported computer criminal behavior: A psychologi-

cal analysis. *Digit. Investig.*, *3*, 116–120. Retrieved from http://dx.doi.org/10.1016/j.diin.2006.06.002 doi: 10.1016/j.diin.2006.06.002

Roose, K. (2016). I dared two expert hackers to destroy my life. here's what happened. Retrieved from https://fusion.net/video/271750/real-future-episode-8-hack-attack/

Saroha, R. (2014). Profiling a cyber criminal. *International Journal of Information and Computation Technology*, *4*(3).

Shahani, A. (2015). Major flaw in android phones would let hackers in with just a text. *NPR*.

Shaw, E. D. (2006, March). The role of behavioral research and profiling in malicious cyber insider investigations. *Digit. Investig.*, *3*(1), 20–31. Retrieved from http://dx.doi.org/10.1016/j.diin.2006.01.006 doi: 10.1016/j.diin.2006.01.006

Stanley, J. (2015). *How propaganda works*. Princeton University Press.

Taylor, P. (2012). *Hackers: Crime and the digital sublime*. Routledge.

Timberg, C. (2015). A disaster foretold — and ignored. *Washington Post*. Retrieved from http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of android social-messaging applications. *Digital Investigation*, *14, Supplement 1*, S77 - S84. Retrieved from http://www.sciencedirect.com/science/article/pii/S1742287615000547 (The Proceedings of the Fifteenth Annual {DFRWS} Conference) doi: http://dx.doi.org/10.1016/j.diin.2015.05.009

Whittaker, Z. (2016). Us report confirms ukraine power outage caused by cyberattack. *ZDnet*.

Wiener, R. L., Krauss, D. A., & Lieberman, J. D. (2011). Mock jury research: Where do we go from here? *Behavioral sciences & the law*, *29*(3), 467–479.

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management*, *24*(4), 281–287.

Zdziarski, J. (2014). Tl;dr: Hacked celebrity icloud accounts. *Zdziarski'S Blog*. Retrieved from http://www.zdziarski.com/blog/?p=3783

APPENDIX A

Hacker Perception Questionnaire

For the following scenarios: Hacker is defined as: A person who uses computers to gain unauthorized access to data Hacking is defined as: Using a computer to gain unauthorized access to data in a system.Please answer all questions based on your personal opinion.

1. A movie production company is about to release a highly anticipated movie. A hacker has hacked into the movie production company and gained access to the entire movie. In the above scenario, what is the more likely reasoning for the hacker's actions?
   (a) The hacker did this in order to condemn the film and muzzle their marketing efforts.
   (b) The hacker did this in order to release it free to the public early.

2. A hacker has hacked into the security system of a prison and controlled the system in order to have prisoners escape. In the above scenario, what is the more likely reasoning for the hacker's actions?
   (a) The hacker did this because he believes the prisoners were wrongfully convicted.
   (b) The hacker did this because he wanted to see anarchy from the comfort of his computer.

3. A hacker has hacked into the computer of a suspected pedophile for evidence to give to police. In the above scenario, what is the more likely reasoning for the hacker's actions?

(a) The hacker did this because he/she wants justice.

(b) The hacker did this because he/she enjoys the power that hacking brings.

4. An ex-employee has hacked a CEO of a large corporation to show how much he does not care about his workers In the above scenario, what is the more likely reasoning for the hacker's actions?

   (a) The hacker did this in order to let the world know of the unethical actions of his previous employer.

   (b) The hacker did this in order to get revenge for being fired.

5. A hacker has hacked celebrities' cellphones to share nude photos of the celebrity on the internet. In the above scenario, what is the more likely reasoning for the hacker's actions?

   (a) The hacker did this in order to show the world security issues that have been reported but never fixed for years, finally forcing companies to fix them.

   (b) The hacker did this out of sexual desire.

6. A hacker has hacked a former romantic partner, who broke up with the hacker and is seeing someone else, in order to send anonymous threats to the new romantic partner until the new partner decides to break up. In the above scenario, what is the more likely reasoning for the hacker's actions?

   (a) The hacker did this because the new romantic partner is abusive and feels the need to take action.

   (b) The hacker did this because of his/her selfishness and wants to see his former partner as suffer like he/she did.

7. A hacker DDOSing black market websites that sells stolen credit cards. A DDOS is a defined as: "distributed denial-of-service attack" which is an attempt to make a service unreachable by flooding the system with more traffic than it can handle. In the above scenario, what is the more likely reasoning for the hacker's actions?

   (a) The hacker did this in order to prevent innocent people's credit cards from being sold

   (b) The hacker did this in order to blackmail the site owner into giving the hacker a portion of the profits.

8. A hacker has created a botnet (a botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam messages.) Q16 In the above scenario, what is the more likely reasoning for the hacker's actions?

   (a) The hacker did this in order to mine bit coins (a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank) to then give to charity.

   (b) The hacker did this in order to DDoS attack company/government servers.

9. A hacker has hacked a presidential candidate's twitter account In the above scenario, what is the more likely reasoning for the hacker's actions?

   (a) The hacker did this in order to spread awareness on something the presidential candidate did that was covered up.

   (b) The hacker did this in order to say lewd and inappropriate things for fun on the account.

10. When you hear the word hacker, what do you think?

11. What do you believe hackers are motivated by?

12. When is hacking okay?

13. When is social engineering okay? Social engineering is defined as: psychological manipulation of people into performing actions or divulging confidential information

14. Are hacktivists extremists? Hacktivist is defined as: An individual who is involved in the subversive use of computers and computer networks to promote a political agenda

15. What penalty should someone get for hacking?

16. Please select the degree to which you agree or disagree with the statements below.

    - Disagree strongly
    - Disagree moderately
    - Disagree a little
    - Neither agree nor disagree
    - Agree a little
    - Agree moderately
    - Agree strongly

    You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other. I see myself as

    - Extraverted, enthusiastic
    - Critical, quarrelsome
    - Dependable, self-disciplined
    - Anxious, easily upset
    - Open to new experiences, complex
    - Reserved, quiet
    - Sympathetic, warm
    - Disorganized, careless
    - Calm, emotionally stable
    - Conventional, uncreative

17. What is your age?

18. What is your gender?

    - Male
    - Female

19. How would you describe yourself?

    - White
    - Black or African American
    - American India or Alaska Native
    - Asian
    - Native Hawaiian or Other Pacific Islander

20. What is your current major? (If you are a double major, choose a primary)

21. What is your religious preference?

    - Christian (non-specific)
    - Evangelical Protestant
    - Protestant
    - Catholic
    - Mormon
    - Orthodox Christian
    - Jehovah's Witness
    - Buddhist
    - Hindu
    - Jewish
    - Muslim
    - Buddhist
    - Atheist
    - Agnostic
    - No religious preference
    - Other (please specify)

22. Please write the names of TV shows or Movies you think of when thinking about those that involve hackers: