WHO ARE COMPUTER CRIMINALS?

by

Kevin W. Jennings, M.S.C.J.

A dissertation submitted to the Graduate Council of
Texas State University in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
with a Major in Criminal Justice
August 2014

Committee Members:

Brian L. Withrow, Chair

Bob Edward Vásquez

Jay D. Jamieson

Matthew Draper

Jose R. Agustina

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

DEDICATION

To Hal Jennings, Judy Jennings, and Matthew Draper, for showing me the path.

To Sara Jennings, for joining me on the journey.

ACKNOWLEDGEMENTS

This dissertation never would have been possible without the support of many people who have guided me and cheered me on throughout this process. Dr. Brian Withrow was an excellent chair, and Doctors Vasquez, Jamieson, Draper, and Agustina all did their part in making this paper possible. Thank you for helping me, but even more important, thank you for putting up with me. I also need to give a big thank you to my mentor Dr. Tomas Mijares, who could not be on my committee but helped and guided me throughout the process of learning, teaching, and growing at Texas State University. Thank you.

For my friends, colleagues, and confidants like Dr. Jackie Schildkraut, David Prosser, Michael Polansky, Dr. James Grace, Marcus Carey, Dustin Melbardis, Dr. Kim Yong Suk, Dr. Jennifer Rowland, Andrew Galloway, Aaron Knodel, Jamie Staebell, Barbara Viruet, and Kathy Harding. You have all done way more than your fair share helping me in this whole process, and putting up with me through the stress and the grind. Thank you.

My parents, Hal and Judy, helped me through every step in my education process, from learning to walk to formatting this very paper. I would not be here today without your love and guidance. You were both amazing examples, and I live every day trying to be like you. Thank you.

Most importantly, I want to thank my wife Sara Jennings. For the late night feedings, the hugs, the ability to cry on your shoulder, and for basically running all

aspects of my life outside of school for the last four years. I literally could not have done this without your constant support in all aspects of my life. You are everything I've ever wanted in a wife, a friend, and a partner. I love you.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table **Page**

ABSTRACT

.Computer criminals are compared to non-computer criminals in a 2004 sample of state and Federal prison inmates. Offenders are compared on their age, race, gender, and education. Computer criminals are found to be younger, more white, more female, and more educated than their non-criminal counterparts. Subsets of computer criminals are then compared to each other using the same four demographic variables.

I. INTRODUCTION

Computer crime is a relatively new and misunderstood phenomenon in the field of criminal justice. As computers have become increasingly prevalent, crimes utilizing those computers has grown accordingly. While it was very rare to be the victim of computer crime as recently as a few decades ago, it is now quite common. This increase in cybercrime and cybercrime victimology also corresponds to an increase in cyber criminals, but little is known about who they are, how they think, or what makes them different from criminals who commit more traditional types of crime.

One of the reasons that computer criminals are hard to identify and study is because there is very little agreement as to what the term "computer crime" actually means. Moon, et. al., (2012) define computer crime as "a contemporary, innovative behavioral phenomenon involving the illegal use of computer and computer-related devices by individuals or groups" (p. 460). This definition is loose enough that a bank robber using Google Maps to find a route they wish to take from their home to the bank they intend to rob may be classified as a computer crime. Jaishankar (2011) defines computer crime as "crimes that occur in the cyberspace" (p.xxvii). This definition is tight enough that it excludes any crimes not committed with the use of the internet or other network (cyberspace). To many, the definition of computer crime mirrors the definition of pornography as given by Supreme Court Justice Stewart; "I know it when I see it" (*Jacobellis v. Ohio*, 1964). No matter how it is defined, computer crime is a problem that must be studied if it is to be understood and kept under control. Every citizen of every nation is a possible victim, and the US Secret Service has said that computer criminals

are a threat to "the health and welfare of individuals, corporations, and government agencies… who rely on computers and telephones to communicate" (Halbert, 1997).

One of the reasons that cybercrime has become a problem in recent years is due to the exponential growth of computers in every nation on the planet. While estimates vary, there is somewhere on the order of 1.8 billion personal computers in the world, with that number expected to grow to two billion by 2015 (Winmill, Metcalf, & Band, 2010). The internet has seen similar exponential growth. Only four computers were on the internet in 1969. That number reached 100,000 in 1989, one billion in 2005, and is rapidly approaching two billion (Hoar, 2011). Americans are more connected than most. Over 70 million people in the United States (47% of all households) do their banking online (Winmill, Metcalf, & Band, 2010). 87% of youths in the United States use the internet (Jaishankar, 2011). In other first world countries such as Canada, the numbers are even higher. 99% of Canadian youths use the internet regularly, and 74% of girls from 12-18 years old spend more time in chat rooms than they do on homework (Jaishankar, 2011). This expanded role of computers and the internet in everyday life is increasing the available victim pool for cyber criminals, especially among vulnerable groups like the young.

This increase in cyber criminality impacts businesses in a very negative way. Costs to US businesses have been estimated to be as high as 67.5 billion dollars a year and as much as one trillion dollars worldwide (Winmill, Metcalf, & Band, 2010). Even in 2001, 85 percent of organizations surveyed reported a cyber-security breach, and 64 percent reported monetary loss (Mitnick & Simon, 2002). These figures are increasing and show no signs of slowing. Reported cyber criminality rose 12 percent from 2008 to

2009 and total reported losses increased 212 percent over the same period, and 667 percent from 2001 to 2009. The average loss for each business that becomes a victim of cybercrime is $500,000. One survey of US businesses found that 64.3 percent reported being infected with malware, 29.2 percent experienced denial of service attacks, 17.3 percent experienced some form of password sniffing, and 13.5 percent experienced website defacement. All of these reflect higher percentages than the prior year (Winmill, Metcalf, & Band, 2010).

There have been different methods used to try and reduce cybercrime. In the United States, many laws have been passed which attempt to safeguard information and security in an effort to reduce computer crime. Laws such as the Digital Millennium Copyright Act, Federal Information Security Management Act, the Children's Online Privacy Protection Act, and even the USA PATRIOT Act have provisions to protect data or punish computer criminals (Balkin, et. al., 2007). In 2001, 31 countries came together in Budapest to organize a treaty concerning international cybercrime. The European Convention on Cybercrime has been signed by many European nations, plus the United States, Japan, Canada, and the Republic of South Africa (Balkin, et. al., 2007). This treaty was the first to address international cybercrime issues and has resulted in increased international cooperation with cybercrime investigations and increased standardization for cybercrime law, thereby reducing the number of countries in which cybercrime is legally permitted (Hoar, 2005).

Even with the laws and regulations in place, cybercrime is still difficult to prevent or prosecute. One of the main reasons for this difficulty is that cybercrime is one of the only crimes where the perpetrator can be in one legal jurisdiction, the victim in a second

jurisdiction, and the scene of the crime in a third jurisdiction. In effect, every place on the internet is equally distant from any other point on the internet, making physical or geographic boundaries irrelevant. This multi jurisdictional complication is not a rarity; in more than half of all internet fraud cases the criminal and the victim live in different places (Hoar, 2005). This problem gets more complex if the criminal decides to use intermediaries in more jurisdictions (Balkin, et. al., 2007). Even when the crime takes place in the same jurisdiction where both the offender and victim live, the law is not always clear about what is legal or illegal and what rights the police have in investigating digital crimes (Balkin, et. al., 2007).

Another factor making cybercrime difficult to prosecute is the extremely low rate of reported victimization. A large number of computer crimes are never detected (Jaishankar, 2011). Because of the nature of how a computer system works, a criminal can infiltrate a system and take whatever information they please, and the victim may never even know the criminal was there. Unlike a bank robbery or a car theft, there is no physical property that the victim is being denied. A person whose identity is stolen, who has proprietary or secret information stolen, or who has malware installed on their computer may never know that those crimes happened. Even when people do find out they have become a victim of a cybercrime, they are unlikely to report it (Jaishankar, 2011). The amount of monetary loss in any one cybercriminal act is often very low, so people are less likely to notify police.

Digital evidence can also be very hard for police to obtain. There are no fingerprints, no shell casings, no stolen property they can recover and trace, and no eyewitnesses. Even if evidence of a perpetrator is found, that evidence very commonly

shows only that a certain computer was used or the criminal was at a certain location, and cannot be used to identify a particular person as the criminal (Balkin, et. al., 2007). A chat room conversation between two people may be easy to find if the police can subpoena the information from the chat room's owners, but linking those two online aliases to actual people is extremely difficult (Winmill, Metcalf, & Band, 2010). If the police find a name linked to an account (such as an e-mail account) this may not be accepted as evidence in court because of the easily modifiable nature of digital evidence (*Victaulic Co. v. Tiemann*, 2007). If evidence can be obtained, it is often very difficult for the prosecutor to explain it in such a way that the judge and jury understand what that evidence actually shows (Winmill, Metcalf, & Band, 2010).

The lack of reported victimization and the difficulty in obtaining and using evidence results in a low number of computer criminals being identified. This makes the quantitative study of computer criminals extremely difficult. Another challenge with studying computer criminals is a lack of consensus on the terminology involved. The term "hacker" means different things to different people. In the early days of computers, the term "hacker" was given as a compliment to describe someone who could find creative and efficient solutions to computer problems that others could not solve (Thomas, 2002). More commonly, the term hacker is used as a pejorative. Hackers are thought to be criminals who use their computer skills for illegal purposes (Levy, 2010). Other terms (such as "cracker," discussed later) are also not clear, and the definition of the term may change depending on who is speaking. For the purposes of this work and for ease of understanding, Unless otherwise noted, the terms "hacker," "computer

criminal," and "cyber criminal" are used interchangeably, as are the terms "computer crime" and "cyber crime," despite others claiming those represent differing definitions.

What is agreed upon by computer criminals, law enforcement, and academics is that hackers have a culture that is unique to the computer underground (Thomas, 2002). One of the main influences on this culture is the fiction of William Gibson. This author coined the term "cyberspace" in his novels, which centered around young but very smart hackers who fight against the forces of evil, embodied by corporations and organized crime groups (O'Neill, 2006). These books see the first appearance of many modern hacker stereotypes, including their fashion sense and their lexicon. Other pieces of popular culture influenced hacker culture in other ways. The works of Heinlein, Dick, Asimov, and Ellison also influenced modern hacker culture, from their vocabulary to their obsession with access to information (Thomas, 2002, Levy, 2010). In addition to the social aspects of hacker culture, they also share certain political and moral values (Nissenbaum, 2002).

This work is an attempt to discover what makes hackers different from other criminals. To quantitatively examine what makes those who commit crimes on computers different from those who commit other crimes. Chapter 2 is a literature review that is split into three main sections. The first discusses the history of hackers and how that history affects modern day hacker culture. The second section discusses the more common crimes and techniques that computer criminals can use to accomplish their goals. The third section is a discussion of what previous research has shown about who hackers are, how they think, and why they become hackers. Chapter 3 is the proposed methodology for the current study, which describes the sample and dataset that will be used for

analysis, the variables to be used, and the proposed use of logistic regression to see which of the independent variables has a statistically significant effect on the dependant variable. Chapter 4 is the results section, giving a detailed description of the results of the analysis plan from Chapter 3. Chapter 5 is the discussion section in which the results are interpreted and put in context. Chapter 6 is the conclusion of the study.

The overall lesson from any study on cybercrime is that computer crime is a very serious social ill. While these crimes can be as minor as vandalism, hackers also have the ability to cause real world disasters, including crashing planes, shutting down power grids, and sinking ships (Nissenbaum, 2002). The threat from hackers is so serious that some have proposed a sentence of life in prison for habitual computer offenders and three in four workers believe employers have the right to monitor employee e-mail in an effort to reduce computer crime (Nissenbaum, 2002). There is little to no warning before they attack (Balkin, et. al., 2007) and they are incredibly adept at spotting outsiders and foiling undercover sting operations (Verton, 2002). The threat posed by cyber criminals must be understood before it can be effectively curtailed. Unfortunately, one of the factors that makes hackers so hard to catch is one of the same things that often draws them into the culture of cybercrime in the first place: computers don't judge.

II. A REVIEW OF THE LITERATURE

History

Computer crime began at the Massachusetts Institute of Technology (MIT) in the 1960s. A group of students known as the "Tech Model Railroad Club" (TMRC) due to their hobby of building model railroads began to explore the universities newest computer: a TX-0. Previous computers were giant IBM machines that required punch cards for input and output. This necessitated computer specialists to take the stack of cards from the programmer, feed it into the machine, run the program, and then hand the output back to the programmer. The "users" of these punch card computers rarely even saw the computers, let alone actually used it themselves. The TX-0 was different, in that the user actually interacted with the machine. This machine was fascinating to the TMRC, who had spent their previous years using wires, switches, and "logic elements" to control their model railroad. Soon after the introduction of the TX-0, the TMRC group was obsessed with the world of computers (Levy, 2010).

They began programming for the TX-0 (and its successors) and tinkering with the internal mechanical workings to improve performance or add functionality. When they needed a term to describe the elegant solutions they found for complex computer problems, they used the term "hack", a term that had been used at MIT to describe elaborate college pranks (Levy, 2010, p. 10). The TMRC changed the meaning of the term to describe a feat of ingenuity, style, and ingenious problem solving with a computer. "Hacks" were now clever solutions the group used to accomplish their goals. Any computer user who routinely accomplished these hacks was referred to as a hacker.

The hackers were the elite members of the MIT computer science department, the ones known for accomplishing goals that were thought to be impossible (Levy, 2010).

These early hackers are the source of many modern day "computer nerd" stereotypes. They stayed up for days at a time hacking a program and had no regard for whether it was day or night when they slept. They had little care for themselves, which included both fashion and personal hygiene. They ate copious amounts of junk food. They had little to no social life outside their circle of hacker friends (Nissenbaum, 2002). Because of these factors, they were isolated from the rest of MIT and the rest of society in general. This did not bother them, as it left them more time to hack and more ability to concentrate on computers and programming.

These hackers developed a philosophy that they lived by known as the "hacker ethic." It was a set of rules that the hackers believed (from their experience working with computers) would create the ultimate meritocracy. These ethical rules were never discussed or written down; they evolved naturally and were silently agreed upon by the hackers. The first rule was that "access to computers – and anything that might teach you something about the way the world works – should be unlimited and total" (Levy, 2010, p. 28). The hackers believed that anyone who had the ability to improve some system in the world should have access to that system. Any barrier that keeps someone from that access is inherently bad.

If a hacker saw a system which was not operating at maximum efficiency (such as the Department of Motor Vehicles) then the hacker believed he had the inherent right to fix the system. If his system was better than the previous system, it would be adopted and thus the world would be improved. If it wasn't better than the previous system, it would

be rejected and the next hacker to come along would have their chance at improving the system. It was this rule that led the MIT hackers (who were otherwise law abiding and honest) to break into offices on campus to obtain the tools and information that the school had attempted to deny them. No matter what the school tried, from locked doors to safes, the hackers were always able to get the tools and information they needed to improve the computer system. When it became obvious that the school could not keep them out, the authorities just let them have access to whatever they wanted as long as the hackers didn't tell anyone, in order for the school to save face (Levy, 2010).

The second rule in the hacker ethic is "all information should be free" (Levy, 2010, p.28). Hackers needed access to all the applicable information if they were to improve a system. If they didn't have all the possible information, their attempted improvements to the system wouldn't be the most efficient, effective improvement that they were capable of. When it came to programs, this meant that all software created by any of the hackers was available to everyone. This kept new users from having to redo work already done by a previous user. In the hacker mind, this free flow of information was necessary for any system to function at peak efficiency (Levy, 2010).

The third rule in the hacker ethic is "Mistrust Authority – Promote Decentralization" (Levy, 2010, p.29). Hackers were vehemently anti-bureaucracy. They felt that any organization should have no boundaries and no hierarchy. An open, organic system would allow a hacker free access to the tools and information they need to improve the world. If there were barriers to those tools or information (such as a boss/manager, arbitrary rules, etc.) then the hacker's ability to improve the system would be threatened. Hackers should be free to explore and tinker, because it is only through

this process that the system can be improved. In the eyes of the Hackers, the antithesis of this ethical rule was IBM. IBM was the company that made the computers which the user had no access to. They were the ultimate in bureaucracy and hierarchy, with computer programmers derogatorily called “priests” and “sub-priests” by the hackers (Levy, 2010).

The fourth rule of the hacker ethic is “Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position” (Levy, 2010, p.31). Hackers viewed age, race, etc. as superficial. All that mattered was how good a person was at improving systems. If someone could program that was more efficient than the previous program, they were someone who mattered. If they couldn’t improve a system, they didn’t matter. This rule is best illustrated by the story of Peter Deutsch. He was a local 12 year old who heard about the computers at MIT and came to see how they worked. He soon became obsessed with computers and spent every spare moment in the computer room at MIT. Because he was not a student, he could not sign up for computer time on his own. He solved this problem by finding students who were having trouble solving some programming dilemma and offering to help. Peter bargained with the programmer by negotiating that if he fixed the programmer’s problem, the programmer would give Peter the rest of his scheduled computer time. He never failed to solve the problem within a few minutes and had the rest of the scheduled time on the computer to hack. The hackers who actually went to MIT accepted him as one of their own, barely even noticing that he was only 12 years old (Levy, 2010).

The fifth rule of the hacker ethic is that “you can create art and beauty on a computer” (Levy, 2010, p. 31). Programming was considered by the early hackers to be an art. The code for any given program held a beauty of sorts, and some programs were

more beautiful than others. If a person could write a calculator program for a computer, they were a programmer. If they could write a beautiful calculator program, they were a hacker and an artist. The early computers had extremely limited amounts of memory, so the shorter a program was, the more efficient it was. Hackers would spend hours trying to find innovative and beautiful ways to make programs shorter. It wasn't a job, it wasn't a competition, "it was a quest" (Levy, 2010, p.33). In addition to this inherent beauty in any efficient and effective computer program, some of the earliest computer programs were art of another sort. Some early programs made the lights on the outside of the computer itself blink on and off in interesting patterns. As soon as a piece of hardware was added to the computer that could make noise, hackers made that hardware play rudimentary music. Whether the hacker was working on a program to make music or a program to make a more memory efficient program, they (and their fellows) were considered artists (Levy, 2010).

The sixth and final rule of the hacker ethic is that "computers can change your life for the better" (Levy, 2010, p. 34). While this is generally accepted today, back in the 1960s it was rare to find someone who could envision how computers may be able to help normal people. They were seen as tools for universities and governments, not tools for helping regular people. These early hackers saw how computers could improve many aspects of everyday life. One notable example was the first computer game, Spacewar. This game (similar to the more modern game Asteroids) developed an entirely new mode of entertainment that is a multi-billion dollar industry today. On a more abstract level, hackers viewed the hacker ethic itself as a way that computers could change the world for the better. Computers had led to the rise of hackers, hackers had created the hacker ethic,

and the hacker ethic was (to the hackers) the ultimate philosophy on how to live. If the world were run by the hacker ethic, it would soon become a meritocracy and a utopia, freeing the world from the burden of inefficiency (Levy, 2010).

Because of the fifth and sixth rule of the hacker ethic, these early hackers felt the need to show people that computers were not a threat, as most non-users seemed to believe. Because the vast majority of money to build and study computers came from the military, computers were seen as tools of war. Public perception of computers was very negative. The hackers wanted to remove that threatening feeling from computers and show the world that computers were harmless. They wanted technology to be seen as a benefit to society, not as a tool of warfare and oppression. They wanted to make sure that technology was never used to harm humans, only to help them. This was exceedingly difficult because most of the early hackers were funded either directly or indirectly by the Department of Defense (Thomas, 2002).

Another impact of the hacker ethic was that computer code was not seen as property. The idea of royalties or copyrights for software was an unheard of concept with the early hackers. They would make a program and then give it to everyone to use and improve upon, and only by giving away the original code of the program could other hackers have the ability to change that code and make that program more efficient. Hackers did not keep secrets from each other. Everything was done with an eye towards the hacker ethic, which means that all hackers had all the information they would need to improve the program. If someone from another university or a computer business called and asked for a copy of a program, the hackers viewed this as an incredible honor and a

sign of their superior programming skill. There was never any question of charging money for the requested program (Thomas, 2002).

Besides the hacker ethic, another world-changing idea in the field of computers emerged from MIT in the 1960's. J.C.R. Licklider had the idea of connecting computers all across the globe into a giant network, allowing for instant access of information from anywhere on the planet. This was the intellectual birth of the internet (Jaishankar, 2011). By the late 1960's, the idea had been picked up by the Department of Defense's Advanced Research Project Agency (ARPA or DARPA). They decided to develop what became known as the ARPANet. Originally, the ARPANet connected only four computers, one each from the University of California – Los Angeles, the University of Utah, Stanford, and the University of California – Santa Barbara (Winmill, Metcalf, & Band, 2010). The universities used the network as a method to transfer datasets instantly from one university to another, allowing data analysis to be shared between universities in a practical way for the first time. The military wanted to build the ARPANet because it was an advanced communication system that would remain functioning even after many pieces of the network had been destroyed, thus it was a system that would continue to function long after others methods of communication had failed in the event of a nuclear war (Hoar, 2005).

The ARPANet was built with the hacker ethic in mind. It was decentralized, meaning that there was no control center or central hub that could fail and take the entire system down with it. It was designed specifically so that there was no hierarchy. Any node or computer on the network was just as important as any other computer. This design encouraged the free flow of information and encouraged exploration. A hacker

from anywhere in the country could sit at a terminal and work on a computer hundreds or thousands of miles away (Levy, 2010).

In the 1970's, it became possible to have a computer in one's own home. A small number of hackers were able to make their own home computers, but the first commercially available home computer was the Altair 8800. The Altair was not a home computer as we think of them today. The purchaser would send a check to the company, and would receive a box with a collection of computer parts. The user would have to assemble the computer themselves. If the user was an experienced engineer, this process would take about 40 hours. If they weren't an experienced engineer, it could take much longer. Once the computer was assembled, it did little more than turn on and off. It was only a processor in a box with 256 bytes of memory and some switches. There was no monitor or output device of any kind besides a few small lights, and there was no mouse, keyboard, or any other input device besides the few switches. If the user wanted it to do something, they had to design and build any hardware that was required and then write the program to accomplish that task by themselves (Thomas, 2002).

Other companies made home computers with improved ease of use and more features, but the first widely successful, easy to use home computer was the Apple II, introduced in the late 1970's by a company called Apple Computer. This company had been started by two hackers named Steve Wozniak and Steve Jobs, who wanted to make the ultimate home computer in order to take the hacker ethic out of the universities and into people's homes (Levy, 2010). These newer, more user friendly home computers saw a huge rise in the number of sales in the late 1970's, and 724,000 home computers were

sold in 1980 alone. In 1981, IBM decided to join the home computer market and that year sales reached 1.4 million units industry wide (Winmill, Metcalf, & Band, 2010).

The huge rise in home computers and the development of computer modems with which computers could communicate with each other over phone lines created an entirely new generation of hackers. The internet was still a tool for universities and governments, so hackers had to make do with what were known as Bulletin Board Systems (BBS). This was similar in function to a miniature internet, where a computer user could dial in and find e-mail, forums, games, and other resources. The difference was that very few computers (in many cases, only one) could be connected at any one time. One user would dial into the BBS, write an e-mail to a second user, then would have to log off in order to free up the BBS's modem so the second user could dial in, receive the e-mail, and write a reply. In addition, each BBS was separate. A user of one BBS could not send an e-mail to a user of another BBS. This, combined with the large cost of long distance phone calls to connect to non-local BBSs, drastically reduced the user base to the point where even the largest BBSs only had a few hundred users (Thomas, 2002).

Hackers used these BBS systems to communicate and share knowledge of hacking. There were numerous BBS systems set up to share hacker programs, gossip, learn the newest tricks, and share stolen credit card numbers and passwords (Winmill, Metcalf, & Band, 2010). A new magazine called Phrack was started in 1983. This electronic only publication combined the words "phreak" and "hack" and was used as a hacker guide to the underground. Hackers also had a hard copy magazine called 2600, which referred to the 2600Hz tone used by hackers to hack the phone system (Thomas, 2002). These publications, combined with BBSs, spread the hacker ethic and hacker

knowledge to an entirely new generation of hackers who could now sit and hack from their own bedroom.

This period saw an increase in computer deviance, so for the first time, Congress passed a major piece of legislation targeted specifically at computer crime. The Computer Fraud and Abuse Act (CFAA) of 1986 was originally intended to protect classified information and financial information on government computers. It also had protections for private financial and credit information on Wall Street computers. The act only protects computers from criminal acts in which there is a "compelling federal interest" (Winmill, Metcalf, & Band, 2010, p. 25), and it did not apply to criminal acts perpetrated by minors, so the ability of the police to prosecute under the CFAA was limited. In the intervening years, these limitations have been, for the most part, removed by subsequent amendments to the CFAA (Winmill, Metcalf, & Band, 2010).

In 1986, a hacker going by the alias The Mentor published The Hacker Manifesto in the magazine Phrack. It was a short essay about the world of the hacker, and how society views all hackers as children, as deviants, as criminals, and as "all alike." The manifesto ends as follows:

> This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.
>
> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging

> people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
>
> I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike. (Blankenship, 1986, p.1)

This manifesto was a rallying point for the new generation of hackers. It united the 1980's hackers into a common collective and inspired them to become an even more cohesive underground society. Only hours after the manifesto was written, the author, Lloyd Blankenship, was arrested for hacking (Olson, 2012).

It was around this time that the internet started to see its first crimes. In the mid 1980s, the internet was still mostly for governments, universities, and large corporations. In 1986, a well publicized incident happened in which an international intrusion into American computers was detected. Only two years later, the first large internet worm was released on the internet. The Morris worm infected computers so swiftly that it took down approximately ten percent of the 88,000 computers that existed on the internet at that time. It was estimated to cost over $100,000 in damages (Hoar, 2005).

Hacking in the 1990s changed. Due to lowering prices and increased ease of use, more people than ever before owned computers. Even small companies were beginning to move a wide array of business processes onto networked computers. Most of these computers had rudimentary security at best, and in many cases no security whatsoever. This led to a target rich environment for hackers. Millions of new subscribers flooded the internet, and hackers found in the internet a system that they could hack in new ways. With 16 million computers on the internet by 1995 (Winmill, Metcalf, & Band, 2010) hackers had a functionally unlimited number of potential hacking targets from which to choose. Hacking also became more public, as the internet allowed hackers enough of an

audience that they began to advertise and brag about their hacking exploits online by posting evidence of high profile intrusions and data thefts from major corporations. Posting proof of the hacker's ability on the internet for everyone to see became a way for hackers to gain reputation and prestige among the growing hacker community (Thomas, 2002).

This explosion of computer crime also saw a corresponding rise in civilian demand for law enforcement attention to computer crime. As law enforcement started to pay attention to the increased criminality being committed with computers, they stepped up enforcement of the newly passed cyber crime laws. In May of 1990, the US Secret Service launched Operation Sundevil, which was one of the largest anti-cybercrime operations of the era and is still one of the most famous anti-cyber crime operations. 27 search warrants were served in 14 different states, but only three arrests were made. It targeted a specific group of hackers who had been working together to steal information from BellSouth, the telecommunications company. Today, this operation is regarded by most to have been ineffective against cybercrime except as a message to cybercriminals. It was a way for the Secret Service to tell the hacker community that law enforcement was going to start taking computer crime more seriously, and that they had the resources to investigate and prosecute hacker groups (Halbert, 1997).

One of the most influential events in the history of hacking happened in August of 1991. Linus Torvalds created a new operating system called Linux. While most people continued to use operating systems developed by Microsoft, Linux was immediately adopted as the unofficial hacker operating system. Linux was based on the hacker ethic from the 1960s. It allowed complete and total control over every aspect of the operating

system. The user was able to see the code and modify it as they saw fit. All modifications for Linux were written by users and then shared over the internet for any other hacker to find, use, and modify further. It gave the user absolute, complete control over everything that was happening within their system, and because it was open source software, Linux was available for no monetary cost.

The hacker community had an open hatred of Microsoft, because of the way that Microsoft treated the end user. The Windows operating system was not as open and customizable as Linux. It would not allow the user to modify any substantial part of the operating system. If a security hole was found in Windows (and many security holes were found) the end user could not plug the hole themselves. They had to wait days, weeks, even months before Microsoft put out a patch designed to fix that hole. Microsoft was the antithesis of the hacker ethic. To the hackers, it was everything that was wrong with the modern computer industry. They eschewed Windows and used Linux, which was seen as the perfect hacker operating system, designed and built without any corporate influence to guide its development and distract from what the hacker ethic dictated (Thomas, 2002).

One of the more formative events in hacker culture was the release of the film *Hackers* in the mid 1990s. *Hackers* did more than any other film before to display what it was like to be a hacker, and (more importantly) what people thought it was like to be a hacker. In the film, hacker style is about a person's relationship to technology through music, clothing, appearance, and even their person. It shows that humans themselves are essentially "technological creations" (Thomas, 2002, p. 162). This film reached and influenced millions of young hackers at a time when computer use (and thus computer

crime and hacking) was increasing at a very high rate thanks to the introduction of the World Wide Web, which was a way to make the internet far more user friendly than it had been when it was exclusively inhabited by universities and governments (Thomas, 2002).

It was in 1995 that the most famous hacker in computer history was finally arrested in North Carolina. Kevin Mitnick had been a hacker since the 1980's, and had been on the run from the law for years before he was finally caught. His exploits ranged from pranks such as hacking into drive through window speakers and intercepting 411 (directory assistance) calls to major crimes such as stealing the source code for the VMS operating system and stealing tens of thousands of credit card numbers. Mr. Mitnick was denied a bail hearing and kept in solitary confinement for eight months before his trial, because the justice system believed that his computer hacking skills would allow him to escape from the jail. The prosecutor said in court that Mitnick could whistle into a phone and cause the launch of nuclear weapons, which was a claim that any knowledgeable computer user would know to be false, but the court believed it because of Mitnick's reputation and because the officers of the court were still mostly computer illiterate. It was still not clear what hackers could do in an increasingly computerized society, and these fears and paranoia were used against Mitnick (Thomas, 2002).

In the 2000s, the computer world has become exponentially more complex, but computers have become increasingly easy to use. Advances in software and lower prices have caused computers to become more prevalent and more efficient. They have been seamlessly integrated into a huge array of consumer products. Computers are in phones, cars, televisions, personal data assistants, music players, and many more products. All of

the computers in those products can be hacked by people who are the intellectual descendants of the original MIT hackers. Whereas in the early days computers were the realm of university students and government workers, computers in this century are everywhere, and it is almost impossible to live a life in a first world country without owning computerized devices in some form. This shift in how computers are distributed in society is opening up new ways for hackers to take advantage of people and commit crimes in ways that are increasingly more difficult for consumers to avoid (Thomas, 2002). While many hackers today are still bound by the hacker ethic that was developed in the 1960's, there are other groups of hackers that have created a different ethic or have no ethic at all.

Techniques

Hackers do not all use the same techniques and commit the same crimes. There are many crimes that a computer criminal can commit, and many ways in which they can be committed. The following chapter discusses the more common computer crimes and some of the techniques used by hackers to help them perform those illegal acts. Not all of the techniques listed here are illegal. Many of them have perfectly legitimate uses that criminals have co-opted for illegal ends. In addition, many of the techniques require little to no computer skill (Jaishankar, 2011).

Current US law recognizes at least 30 different computer crimes, which include extortion, internet fraud, credit card fraud, sale of controlled substances, piracy, stalking, espionage, securities fraud, and many others (Winmill, Metcalf, & Band, 2010). Many international laws fail to acknowledge many of these acts as crimes, and focus almost exclusively on network intrusion, child pornography, and economic frauds (Jaishankar,

2011). In addition to these crimes, there are additional legal techniques and tools which are easily adapted by hackers to make their criminal actions easier or harder to trace. These techniques include the use of anonymous remailers and encryption, which make hackers even more difficult to identify on an already heavily anonymous internet (Jaishankar, 2011).

Phreaking

One of the oldest techniques at a hacker's disposal is phone phreaking. This refers to the process of hacking the phone system to do what the phreaker wants it to do. While this may not seem like computer hacking at first glance, there has been a long relationship with phone hacking and computer hacking. One of the most famous phone phreakers of all time was John Draper. He found that a whistle found as a toy in a box of Captain Crunch cereal could be used to reset the phone trunk lines, allowing the phreaker control over the system. Because of this, Draper earned the handle "Captain Crunch" (Winmill, Metcalf, & Band, 2010). This whistle worked because it happened to sound at the exact tone that the phone company used to send commands over the phone lines to their trunks: 2600Hz (Verton, 2002).

The earliest hackers were also some of the earliest phone phreaks. The TMRC at MIT would take tours of phone company facilities like other people might take a tour of a museum. They viewed the phone company's infrastructure as just another system that could be hacked and optimized. Stew Nelson was the first person to combine phone signals and computers when he developed the first computer modem for the PDP-1 system. The hackers would use this device to endlessly explore the phone system both in the United States and Internationally. They would even impersonate phone company

employees and inform the phone company of broken or malfunctioning equipment when they stumbled across pieces of the system that weren't working right. Some of the hackers developed and sold blue boxes, which were simple devices that a non-hacker could plug into a phone line and use to make free long distance phone calls. While some hackers saw this profiteering as a violation of the hacker ethic, others saw it as just another hack of the system. Steve Wozniac even used some of the profits from the sale of blue boxes to finance the first Apple computers (Levy, 2010).

The Communications Assistance of Law Enforcement Act of 1994 (CALEA) inadvertently makes the process of phone phreaking much easier. This law states that law enforcement has to have access to the phone system so they can tap and monitor telephone communications quickly and easily once they acquire a warrant from a judge. This prevents the phone company from modifying the phone system to make it harder to hack. The FCC has ruled more recently that CALEA also applies to broadband internet service and Voice over Internet Protocol (VoIP) providers. These legally mandated phone system features that allow law enforcement to wiretap phone lines are breaches in the security that allow phone phreaks unlimited access to the phone system (Balkin, et. al., 2007).

What a hacker does with their control over the phone system is a matter of personal morality. Some hackers use their phone phreaking abilities to explore and improve the system. Joe Magee was a phone phreak in Philadelphia who started exploring the phone system at a young age. When he realized that he had the power to take out Philadelphia's entire phone system at will, he called the phone company to inform them of their vulnerability. He was shuffled around from person to person and

was told that he was being “silly” (Verton, 2002, p. 48). Other hackers purposefully bring down the system, such as the Masters of Destruction (MOD) hacker group did in 1990. They sent bad commands to the phone companies routing system and took down a huge portion of the phone company network, preventing about 75 million phone calls from taking place. Both moral choices (tell the phone company about the problem; crash the system) can be justified by the hacker ethic. Both Joe Magee and the MOD would claim that they had explored the system, figured out how it worked, found the flaws in that system, and then did what they could to inform the owners of that system about what those flaws were. The MOD would claim they just used a more direct and memorable method of accomplishing the same goal that Joe Magee was trying to accomplish (Verton, 2002).

One of the most famous Phone phreaks of all time was Kevin Mitnick. In addition to his computer hacking skills, he was an accomplished phone phreak and used the phone system to his advantage in his other exploits. As a young man, he would prank others by rerouting calls intended for directory assistance to his own personal phone number. He would give the callers wrong numbers or impossible to dial numbers (Five five five, four one-half one two) as a way to have fun when he was bored (Mitnick & Simon, 2011). He and his phone phreak friends would also give themselves the Caller ID service before it was legally available from the phone company, and would surprise their non-phreak friends by answering the phone knowing exactly who was on the other end of the line (Mitnick & Simon, 2002).

Later, when he was on the run from the police, he used his phone phreaking skills to make himself much harder to catch. He hacked a cell phone so that he could call other

numbers anonymously. This also allowed him to have free and untraceable cell service so he could contact his family and friends without law enforcement being able to track him (Mitnick & Simon, 2006). He was also able to route his phone calls through many phone trunks set up in many different cities, making his calls extremely hard to trace. After he was arrested, he was able to manipulate the jail phone system to talk to people other than his lawyer (Mitnick & Simon, 2011).

War Dialing and War Driving

Phone phreakers often used a technique called "war dialing" in which a modem was set to dial every possible number in a certain prefix and record which numbers were answered with modem tones (Thomas, 2002). So, for instance, a hacker would set their modem to dial 512-555-XXXX, and the computer would dial every possible combination of phone numbers within that range and find all of the modems that were hooked up to those phone lines. This would give the hacker a long list of possible hacking targets. War dialing programs could only dial about one hundred and fifty numbers an hour, but this was one of the main ways for hackers to find hacking targets before the days of the internet (Levy, 2010).

Since the late 1990's, the number of dial up modems has decreased dramatically as broadband internet connections became more popular. War dialing is nearly extinct as a hacker technique, but it has been replaced by war driving, which is a similar technique utilizing wireless networks. A war driver will set up a laptop computer or other mobile device to read and record any wireless networks it encounters, and then drive, walk, or bike around a city or suburban area. The laptop will record every detected wireless network, including its broadcast strength, name, security settings, and geographic

location. With this list, a hacker can easily find a wireless network that is either unsecured or easy to hack into that is accessible from a public place. A hacker will then use these networks to mask their location when performing certain illegal acts. For instance, if a hacker wishes to download contraband hacking programs from a website that they think may be under law enforcement surveillance, they can travel to one of the open networks found by a war driver, connect to the unsecured network, and download software, media, or other digital information from anywhere on the internet. If law enforcement is watching the site or gains access to the site's records after the fact, they will trace the download to the owner of the unsecured network, who has no connection to the hacker who actually downloaded the contraband programs (Balkin, et. al., 2007).

Malware

Malware is "destructive software designed to damage, disrupt, alter, or steal data" (Hoar, 2005, p. 1). There are many types of malware, including viruses, worms, trojans, and ransomware. The most common types are viruses and worms. These are programs that infect computers and then propagate to other computers, infecting populations of computers like normal viruses infect populations of humans. The difference between the two is a matter of some debate, but the most common delineation is that worms can spread from computer to computer without any human interference while viruses require some sort of (usually inadvertent) action by the human operator of the computers it is infecting (O'Neil, 2006). There is also spamware which puts spam commercial messages onto a user's computer (O'Neil, 2006) and trojan horses, which is malware connected to a useful program that the user downloads and installs, thereby installing the useful program

that they intended to install and the trojan horse program the hacker wanted them to install as well (Thomas, 2002).

There have been many famous (or infamous) viruses and worms. The 1988 Morris worm was the first major worm to infect large numbers of computers connected to the internet (Thomas, 2002). In 2003, the Sapphire (also called Slammer) worm was released. It was the fastest spreading worm in computer history, doubling in size every 8.5 seconds. It infected at least 75,000 computers, but probably much more (Balkin, et. al., 2007). The Melissa virus attached itself to Microsoft Word documents and spread itself via Microsoft's e-mail programs and caused over 80 million dollars in damages to worldwide business interests whose computers or e-mail servers were taken down by the virus (Jaishannkar, 2011). The number and impact of viruses and worms continues to grow, with new viruses like the Love Bug, Code Red, MyDoom, Klez, and SoBig being released every year. In 2004, over 115 million computers were infected by 480 new pieces of malware, and this number is growing every year (Hoar, 2011). Virus writers have become so proficient and so prevalent that Microsoft has begun offering bounties for information leading to the capture of certain virus writers (O'Neil, 2006).

Malware has become increasingly effective in recent years. Part of this is due to a Darwinian "survival of the fittest" scenario in which anti-virus programs and increased awareness and security have weeded out the less effective viruses, leaving the powerful to thrive (O'Neil, 2006). In addition, there is the increased danger caused by digital monoculture. Even with the introduction of Linux and Apple operating systems, the vast majority of people in the world today use the Microsoft Windows operating system. This makes the job of the virus writer much easier, because he or she only has to worry about

how to make their virus affect one operating system in order to ensure a wide spread of infections. Other pieces of software that a virus can target are also becoming increasingly standard. Web browsers, word processors, instant messengers, and many other forms of software have one (or a small few) options that the vast majority of people all use (Balkin, 2007).

This increased efficiency of viruses and the increased reliance on computers has resulted in companies being especially vulnerable to malware. A 2009 survey found that 64.3% of businesses were infected by malware during the year, compared to only 50% the year before (Winmill, Metcalf, & Band, 2010). These malware infections can cause loss of data, identity theft, fewer customers due to security fears, and losses stemming from the time needed to clean the machines of the infection (Jaishankar, 2011). One estimate says that US computer users spent 7.5 billion dollars to repair or replace computer systems that had been infected with malware (Nykodym, et. al., 2010).

The people who write viruses and other malware are nearly universally hated by the non-hacker community. There are very few people who actually create serious viruses, however. The amount of people with the combination of skill and motivation to create a virus that will be effective is very low. In 2004, there was one person who created two very successful viruses and was therefore responsible for 70% of all the worldwide virus infections that year (Balkin, 2007). On the other hand, there are tangential benefits to malware. They are able to quickly and easily point out the security flaws in many systems in a relatively safe way. If those flaws were found by someone wishing to do serious harm, they could very easily be used to create much more serious financial and physical damage (O'Neil, 2006).

In the future, viruses and other types of malware will continue to become more complicated and more effective. Already, there are worms that can infect cell phones (Hoar, 2005). A new type of virus called a "polymorph virus" can change itself every time it infects a new computer, and can lie dormant on a system that the user thinks has been cleaned of the infection (O'Neil, 2006). Malware makers will find new ways to infect personal computers and any other digital device with viruses, worms, and spamware. While this type of crime can be reduced through the use of anti-virus software and better browsing practices, this problem will continue to exist as long as digital data exists.

Vandals

Websites are not always taken down by malware. Many times, they are taken down by internet vandals who deface, destroy, or otherwise shut down websites or services. 13.5% of American businesses reported some form of website defacement in 2009 alone (Winmill, Metcalf, & Band, 2010). Even the webpage of the United States Senate was defaced in 1999, with the vandal writing "You can stop one, but you cannot stop all" (Nissenbaum, 2002, p. 54), a paraphrasing of a line from The Mentor's Hacker Manifesto. These website defacements and disruptions cost websites millions of dollars a year in lost revenues from advertising on their sites alone (Nissenbaum, 2002).

Most hackers dismiss website defacement and similar acts of vandalism as "not serious hacks" (Thomas, 2002, p. 166) but many argue that the defacement is meant to make a more political or social point. Some hackers go so far as to brag that they never destroy any of the files found on the websites they deface, claiming that this makes it clear they have a moral point to make. They also claim that their defacement is a milder

"punishment" for the crime of having lax security than many other possible actions the hackers could take. In this line of thinking, defacement is a quick, easy, and relatively painless way to teach website owners that they have security holes that need to be fixed (Verton, 2002). Famous hacker Kevin Mitnick disagrees, saying that vandals are only out to inflate their ego and take pride in showing off their juvenile antics to others on the internet (Mitnick & Simon, 2002).

Bot Masters

A botnet is a collection of computers that have been taken over by a hacker. The hacker creates the botnet by writing a piece of malware that is then sent out on the internet to infect machines. When a machine is infected, it runs a program in the background which listens for commands from the hacker and is known as a "bot" or a "zombie." Successful bot masters can have botnets consisting of tens of thousands or even hundreds of thousands of zombie computers. The larger a botnet is, the more prestigious it is for the bot master. These bot masters either use the botnet for their own purposes, or they rent them out to other hackers for an average of $9 per hour or $67 for a 24 hour period (Olson, 2012).

Botnets are very commonly used for sending spam e-mails and for scanning large numbers of computers for security vulnerabilities, but their most famous (or infamous) use is for a type of vandalism known as Distributed Denial of Service Attacks (DDoS). In this type of attack, a hacker uses as many separate systems as possible to send a flood of useless data at a target system. The target system becomes overwhelmed with data and will eventually cease to function. Even if the amount of data being sent at the target isn't enough to crash the entire system, even a moderately large amount of trash data will

severely slow the legitimate users of the target system. The hacker group Anonymous is known to rent botnets and use DDoS attacks to take down websites they have political disagreements with, including the Church of Scientology's website, the Paypal website, and the Central Intelligence Agency website (Olson, 2012). In 2000, a hacker named Mafiaboy spent a week using the botnet he had created to take down sites such as Yahoo, eBay, Amazon, CNN, and E-Trade (Verton, 2002).

Script Kiddies

"Script Kiddie" is a common term used to describe people who hack but don't perform those hacks using their own programs. They download, install, and use pre-made hacking programs written by hackers, but don't truly understand the methods they are using. Hackers view script kiddies as lesser, as not true hackers. They claim that using pre-made programs to hack is akin to stealing a car when the doors were unlocked and the keys were in the ignition (Thomas, 2002). It is these imitators that gave rise to the tradition of hackers having to prove their worth before they are taken seriously. If a self-proclaimed hacker joins a chat room, they are required to prove they are not a script kiddie before they are taken seriously (Verton, 2002).

Script kiddies are well known for performing DDoS attacks. Instead of gathering their own botnet using malware they created, script kiddies download and install premade DDoS software or hire bot masters to do the more technical work for them. These attacks are becoming more prevalent, with 29.2% of US businesses reporting being a victim of a denial of service attack (Winmill, Metcalf, & Band, 2010). Luckily, there are ways to prevent DDoS attacks if the attacker does not have the skills to prevent these defensive measures from being used (a common occurrence with script kiddies). One web hosting

company discovered a denial of service attack being performed against one of their clients, but they found the identity of the hacker and were able to redirect the attacker's data flood back at the attacker's own machine, taking him offline (Balkin, et. al., 2007).

Script kiddies are also known for sending out other types of automated attacks, including spam, viruses, phishing attacks, or other attacks which have been turned into simple point and click programs allowing non-hackers to execute them. The problem has become so great that one company that processes e-mail for large businesses claims that 88% of all the e-mails it processes are some sort of automated attack (Hoar, 2011). The US government is attempting to make these automated attacks less prevalent by passing laws increasing the penalties for violating computer crime laws, but because this type of attack is so easy to perform, it continues to be very prevalent and very lightly prosecuted. Even after the US passed the CAN-SPAM Act of 2003, only thirty people were prosecuted under the provisions of the law within the next four years (Winmill, Metcalf, & Band, 2010).

Social Engineering

Social Engineering is the term used by hackers to describe the ability to manipulate people into giving a hacker the information he wants. Many people call social engineers con-men, but con-men are usually after money while social engineers are usually gathering information for their computer hacking activities. Con-men also usually work face to face, while social engineers very rarely are in the physical presence of the person they are trying to influence. Most social engineering work is done over the phone or over a computer (Mitnick& Simon, 2002). Social Engineering is so valuable to hackers that it has been called the most important skill a hacker can possess (Thomas, 2002).

According to Kevin Mitnick, social engineering involves "becom[ing] an actor playing a role" (Mitnick & Simon, 2011, p.124).

There are many different techniques that a successful social engineer can employ to accomplish their goal of manipulation. The easiest way for a social engineer to gather the information they want is to ask for it. If the social engineer has successfully done their homework, then a straight request for the needed information has a high chance of being successful. First, the hacker must act charming, polite, and easy to like. This will place the target in a better mood and make them more likely to cooperate with the hacker. Second, the hacker must know the lingo that someone requesting the information they want would know. For instance, if a social engineer is calling a phone company line to ask for someone's phone subscriber information, they need to know the correct phone company lingo to use. If they don't, the person they are asking for information may become suspicious. Third, the social engineer must anticipate the questions their target is likely to ask, and be prepared with plausible answers to those questions. These three techniques are even more likely to work on a person who is new to the company or organization that is being targeted, so the social engineer will purposefully attempt to contact a newly hired person (Mitnick & Simon, 2002).

The reasons that a straight request for information has a high chance of being successful if a social engineer follows these three rules is that many companies rely on what's called security through obscurity, which means security that relies on the fact that only certain people know what questions to ask and where/how to ask those questions. For instance, if a phone company has a private line set up for phone technicians to call for information on residential subscribers, anyone calling that number is just assumed to be a

phone technician. A social engineer that finds that number and uses it for their own ends is merely taking advantage of that lack of security (Mitnick & Simon, 2002).

There are other techniques that a person can use that fall under the umbrella of social engineering. One of the more popular ones is tailgating. Not to be confused with the art of drinking beer in a stadium parking lot, tailgating in this context refers to following someone through a door that has an electronic key or PIN system. If the social engineer needs to enter a building but the building's doors have security measures in place to keep out unwanted intruders, the social engineer can just tailgate inside by following an individual with the correct key or passcode, join a large group of people entering the building, or they can get to the door first with a briefcase, box, or something else in their hands and fumble for their (nonexistent) key, which usually induces people following behind to abide by common social convention and open the door for the social engineer (and often even hold it open for them while they enter the supposedly secure building). As long as the social engineer looks like he or she belongs, this technique has a high rate of success (Mitnick & Simon, 2011).

Another technique that is very commonly used is dumpster diving. A social engineer will often crawl into a company's dumpster in order to collect information that is valuable in itself or information that can be used to gain the information the social engineer is after. Kevin Mitnick began his social engineering career by obtaining bus transfer slips from the dumpster behind the bus depot. He also gained valuable information for his phone phreaking activities (such as internal phone company memos, lists of phone company phone numbers, technical manuals, etc.) by dumpster diving at the phone company headquarters. As long as the social engineer is not trespassing, this

action is perfectly legal, as companies do not have a reasonable expectation of privacy in their trash. The experienced dumpster diver will begin his dive by pulling out cardboard boxes and putting them on the ground next to the dumpster. This way, if a security guard or company employee asks the social engineer what they are doing, they can reply that they are looking for boxes because they are moving (Mitnick & Simon, 2002).

A technique that can greatly increase the chance of a social engineering attack being successful is called reverse engineering. In these cases, the social engineer gets the target of the attack to call the attacker and ask for the attacker's help. This can be accomplished in a few different ways, but the easiest method of accomplishing this is for the attacker to create a problem and let the target know that the solution to the problem is the attacker. So a social engineer may call a target impersonating a repair technician of the target company, tell the target that if they have a certain problem on their computer to call the attacker, and then induce the problem sometime later. The target will call the attacker and ask for his or her help to fix the problem, during which the attacker can induce them to install malware on the computer or look up the information the social engineer needs (Mitnick & Simon, 2002).

All social engineering techniques require the use of applied psychology. Psychological triggers are automatic mechanisms that lead people to acquiesce to the requests of the manipulator. Things like fear and gratitude are powerful emotions that the social engineer can manipulate in order to create an emotional state in the target in which they are much more likely to give the social engineer what they want. Social engineers use the same techniques that normal people use every day to gain influence, build credibility, and develop reciprocal obligations, but the social engineer uses these

techniques in a manipulative, anti-social way (Mitnick & Simon, 2006). These manipulations, combined with a perceived authority, allow the attacker to gain the information they are after almost every time. Companies that perform penetration testing of client computer systems report that nearly 100% of all social engineering attacks are successful (Mitnick & Simon, 2002).

One of the most vivid examples of how social engineering can be effective was a study at three Midwestern hospitals in which a man called a nurses station claiming to be a doctor and instructed the nurse that answered the phone to administer a certain drug to a certain patient. The caller was not known to the nurse, the drug was not authorized to be used in that ward, the dosage was twice the daily recommended dosage for that drug, and taking prescription instructions over the phone was a violation of hospital policy. In 95% of cases, the nurses obtained the drug and were on the way to give it to the patient before being stopped by an observer and informed of the experiment (Mitnick & Simon, 2002). In another case, a man named Stanley Rifkin used social engineering techniques to defraud a bank out of 2.2 million dollars with only a few hours work. Luckily, he was caught and prosecuted (Mitnick & Simon, 2002). Most social engineering attacks aren't as spectacular as giving a patient dangerous drugs or stealing millions of dollars. In many cases, social engineers use their skills for much more every day crimes. One hacker would frequently use his social engineering skills to scare young women into taking naked pictures of themselves and sending them to him (Olson, 2012). Kevin Mitnick used his social engineering skills to convince the California Department of Motor Vehicles that he was a law enforcement officer, and received large amounts of information about his friends, teachers, and relatives (Mitnick & Simon, 2011).

Gambling

Hackers have a long history of running illegal gambling businesses or taking advantage of legitimate gambling businesses. Hackers rationalize any theft of money from casinos by portraying themselves as a Robin Hood type character, stealing from the evil casinos who are themselves stealing money from old ladies by getting them to play games that have a fixed advantage for the house (Mitnick & Simon, 2006).

Hackers can easily find a way to cheat with casino games that are supposedly impossible to cheat, such as video poker. A team of three hackers bought a very common brand and model of video poker machine and took it apart in order to find the computer chips with the machine's source code. Once they obtained this code, they found that there was a flaw in the random number generator which they were able to exploit. They were able to take small computers mounted in their shoes into casinos and input any hand they were dealt at the video poker machines. The computer would then tell them the exact instant in which to deal a new set of cards in order to give them the hands they wanted. Each of the three hackers made off with somewhere around half a million dollars before they decided to quit. None were ever prosecuted (Mitnick & Simon, 2006).

Usually, taking advantage of casinos isn't as complicated as buying a video poker machine and taking miniature computers into casinos. One of Kevin Mitnick's associates named Kevin Poulson would use his phone phreak skills to make himself more likely to win radio call in contests. He won two Porches, a trip to Hawaii, and thousands of dollars before being arrested and convicted on other charges (Thomas, 2002). Another hacker created a robot (or "bot" for short) that could play mathematically perfect poker on well known poker websites. The bot he made was so complicated, it could even play in "team

mode" with other bots at the same table. The creator of these bots claims that he never used them to make money, but anything one hacker can do has probably been done by others. It is widely suspected that other hackers have used similar bots on poker sites (Mitnick & Simon, 2006).

More recently, some computer criminals have decided that taking advantage of casinos isn't as profitable as running their own casinos. In countries like Antigua, computer criminals can set up online casinos, allowing people all over the world to gamble in cyberspace. Because the servers are hosted there, the online casinos are able to bypass laws concerning illegal gambling activity in countries like the United States. This circumvention of the law is attractive to criminals of all kinds, and many of the online gambling companies being run in places like Antigua have ties to traditional organized crime who partner with computer criminals to further skew the odds (and profits) in favor of the house. The United States and the World Trade Organization are attempting to diminish the amount of monetary losses to these gambling businesses, but it is difficult to curtail online gambling when the casinos are legal in the country where they are physically located (Jaishankar, 2011).

Crackers

There are many different definitions for what the term "cracker" means amongst computer criminals. The older hackers tend to call any criminally inclined computer user a cracker, to differentiate them from the (mostly law abiding) first generation of hackers (Thomas, 2002). Others contend that the term "cracker" refers to hackers that destroy people's data or entire hard drives (Mitnick & Simon, 2002). In this paper, the term "cracker" will be used to mean a person who breaks computer security. Using this

definition, crackers fall into two main categories. There are crackers that break the security of software and crackers that break passwords (Mitnick & Simon, 2006).

Whenever new software comes out, there are many crackers who are ready to break the security included with the software that is intended to prevent software piracy. Once a cracker figures out that security, he or she can disable it and upload the cracked program to one of several websites that specialize in cracked software (also called "warez"). Crackers will very rarely crack the security on a piece of software and then keep the cracked version for themselves. The cracker who is able to upload a cracked version of any new program first can get a large amount of social capital among the cracker/pirate community. Many advanced crackers will not wait for the software to be released by the company before attempting to crack it. They frequently break into the servers of a company to retrieve copies of the software before it is released to the public. It is nearly impossible to keep a determined hacker out of a large corporate system. If given enough time, hackers will almost always find a way to copy data from any major corporate network that is attached to the internet. Because hackers know how networks are usually set up, they can find and exploit the mistakes that company system administrators are known to make and then steal any data they want off of corporate servers (Mitnick & Simon, 2006).

The second kind of cracker is a hacker who specializes in cracking password files. Passwords are commonly encrypted with a one way hash, which takes the password and puts it through a mathematical process which results in a unique combination of letters and numbers called a hash. It is mathematically impossible to translate that hash back into the password; it is only possible to translate the password into the hash. That is the

reason for using the term “one way” hash. This is meant to increase security by allowing any server to store only the hashes for passwords, not the actual passwords. Every time a user logs in, the server asks for a password and then translates that password into its corresponding hash. If that hash matches the hash on file as the password for that user, the server allows them access. If the hashes don’t match, the user put in the wrong password and will not be allowed access. If the password file is stolen from a server, the thief will not have any useful passwords, he or she will only have a list of useless hashes (Thomas, 2002).

In practice, hackers have found a way past this limitation. A list of hashes is theoretically useless, because a “brute force” attack in which every combination of letters and numbers is put through the mathematical formula and the resulting hash is compared to the known hash can take thousands of years. The problem with this theory is that people do not pick passwords randomly, and thus if the hacker knows how people pick passwords they can narrow down the possible choices. People most commonly pick passwords that they can remember, which makes it very easy for hackers to figure them out (Thomas, 2002). Using a simple program, hackers can put a list of possible passwords through the mathematical formula used for creating hashes and compare those resulting hashes against the password hashes they are interested in cracking. Originally, these word lists were just copies of the English dictionary, which gave this technique the name of “dictionary attack.” Numerous word lists for password cracking are available online, and the larger word lists can crack up to 90% of all user passwords using this method. Even the largest word lists are a tiny fraction of all possible combinations of letters and

numbers, so this method takes only seconds to crack a large number of passwords (Mitnick & Simon, 2006).

The early hackers saw passwords as an affront to the hacker ethic, so they pioneered the practice of password cracking. Passwords only kept hackers from obtaining the information being protected by that password, and thus any computer user who felt the need to use a password to protect their data only aroused suspicion and curiosity from those early hackers (Levy, 2010). This antagonism towards passwords and hiding data is common among modern users as well. In a survey of high school students across the country, 48% said that they thought it was acceptable to crack the computer passwords of fellow students (Mitnick & Simon, 2006). For this reason, it is incredibly important for users to create passwords that can withstand dictionary attacks and for system administrators to protect the password hash files as well as they protect any other sensitive information.

Piracy

In a cybercrime context, piracy does not refer to preying upon wooden sailing ships on the high seas. Piracy is "the illegal copying of digital goods, software, digital documents, and digital audio (including music and voice) for any reason other than to back up without the explicit permission from and compensation to the copyright holder" (Jaishankar, 2011, p. 141). One major economic benefit of digital information is that it has zero reproduction costs. It is incredibly easy to duplicate any piece of information a near infinite number of times. In the real world (what some hackers call "meat space") every item exists in a designated space, and each item has a designated "identity." This

difference makes the world of digital information possible, but at the same time it creates a widespread piracy problem (Balkin, 2007).

One of the first examples of software piracy involved the Homebrew Computer Club in California, which was made up of many early hackers who lived by the hacker ethic. Bill Gates (who would later go on to found Microsoft) coded a version of the popular programming language BASIC for the Altair home computer and started selling it via popular computing magazines. The hackers in the Homebrew Computer Club viewed this software as they viewed all software; information that should be free for all hackers and disseminated as much as possible. They began copying the code and handing it out to anyone who wanted a copy. Bill Gates saw this as theft, and wrote an open letter to the hackers that was printed in many trade magazines calling these software copiers thieves. This upset the hackers and made them even less likely to spend the huge amount of money that Gates was charging for his software (Levy, 2010).

Piracy has only increased over time. A few years after the incident with Altair BASIC, someone pirated the hardware manual for the new Atari game machine. This allowed people to code their own games for the Atari system, and many of these games were then given away to all who were interested (Levy, 2010). Companies started to create copy protection for their software, but other companies created software to get past this copy protection. One popular program called "Locksmith" was marketed as a program intended to let people create backup copies of programs they had legally purchased, but was used to defeat copy protection and pirate games. By the late 1980's, software companies estimated that they were losing half of their business to software pirates (Levy, 2010).

Today, many estimate that software piracy costs companies billions of dollars a year (Jaishankar, 2011). Specific numbers range from about two billion dollars a year (Verton, 2002) to 250 billion dollars a year (Hoar, 2005). The Recording Industry Association of America is attempting to stem the tide of pirated music by suing pirates in civil court. They successfully sued the company behind the software piracy program Napster in 2000 (Warnick, 2004). They pursued legal action against over 30,000 Americans between 2002 and 2008. These lawsuits have been shown to reduce the number of people actively sharing music on the internet, as has increasing the severity of punishment for music piracy (Jaishankar, 2011). As the repercussions for pirating have gotten more severe, pirate servers have moved to jurisdictions in which piracy is not illegal or prohibitions on piracy are rarely enforced. Currently, Russia and the Ukraine have high amounts of piracy thanks to low rates of enforcement (O'Neil, 2006). The problem has grown so large that some are even suggesting that it should be legal for groups such as the RIAA and the Motion Picture Association of America (MPAA) to hack the computers of pirates and install malware on their machines that can prevent them from reoffending (Balkin, 2007).

Many hackers claim that piracy is not morally wrong, or is being blown out of proportion by groups such as the RIAA and MPAA. In the early days of piracy, court cases involved software piracy had to be tried under existing theft laws. These were very rarely successful because hackers successfully argued that piracy was obviously not theft as theft legally requires a deprivation of property from the owner. Piracy does not deprive anyone of anything. It takes a file and makes an entirely new copy that the pirate takes, thus it is not theft (Denny, 2010). In the early days, many hackers argued that it wasn't

piracy if a hacker manually recoded the same program that was available commercially. This has become something of a moot point, as programs today are so complicated that it would be virtually impossible for private citizens to recode them (Levy, 2010).

Most of the arguments against the traditional view of piracy surround the cost. Many of the people who become software pirates are people who don't have large amounts of money, such as college students (Moon, et. al., 2012). Many of these pirates explain that they would like to pay for the software, but the costs to purchase the software or media legitimately are seen as exorbitant and thus the person resorts to piracy. When Bill Gates' version of Altair BASIC was being sold for 150 dollars, it was rampantly pirated. A hacker decided to prove that people would be more willing to purchase the software legitimately if it was sold for a more legitimate price, so he coded his own version of BASIC for the Altair and sold it for five dollars. Within days he had received numerous orders, with some people sending him more than five dollars because they thought five dollars was too cheap, and others sending him money and telling him not to bother shipping them a copy of the program because they had already copied it from a friend (Levy, 2010).

Software companies usually claim that if they do not charge high prices for software, this will stifle software innovation through a lack of financial reward. If software companies are not making money through the sale of their software, they will cease to innovate and create new and interesting pieces of software or media. Hackers and pirates point out that software and media is constantly being made by people with no financial motive. There are numerous pieces of open source software that are seen as equivalent or superior to expensive, mass produced software. Programs like Linux, VLC,

Firefox, and Open Office all show that software can be both innovative and free. Many musicians not only allow their music to be copied and distributed by pirates, but even encourage it. These artists and software engineers either don't want money for their work or they feel they make enough money in other areas besides software/media sales (Nissenbaum, 2002).

Whatever the future of piracy holds and regardless of whether piracy is seen as morally justified or not, pirates contend that current estimates of industry losses due to piracy are completely overblown and exaggerated. They contend that the math used to estimate the financial impact of piracy relies on many assumptions that just aren't true. For instance, many of the estimates assume that any person who downloads the software will share it with others, resulting in an exponential increase in the estimated costs of that one pirate. Almost all estimates assume that the pirate would have bought the software if they hadn't been able to pirate it, which pirates see as an absurd claim. Many pirates claim that they don't have any financial impact on companies because if piracy was not an option, the pirate would not have purchased that piece of software. They contend that the companies will make the same amount of money (zero dollars) from the pirate whether they are able to pirate that software or not. This mis-estimation of costs was displayed in the case of Craig Neidorf, who was accused of downloading software from Bell South that the company estimated was worth almost $80,000. The case was thrown out when the defense proved that every single piece of data downloaded from the Bell South computers was publically available for $13 (Halbert, 2001).

Bullies and Stalkers

Cyber stalking is "the use of the internet, e-mail, or other electronic communication device to create a criminal level of intimidation, harassment, and fear in one or more victims" (Jaishankar, 2011, p. 278) and cyber bullying is "willful and repeated harm inflicted through the medium of electronic text" (Jaishankar, 2011, p. 360). There are many crimes which can fall under the general umbrella of cyber stalking or cyber bullying, and the two categories overlap to some degree. The list includes verbal abuse, defamation, impersonation, harassment, domestic violence, blackmailing, and more. While these crimes are very similar to their non-cyber counterparts, one obvious difference is the lack of required geographic proximity in cyber stalking and cyber bullying. Where the traditional forms of those crimes require the offender and the victim to be in the same place at the same time, the internet allows the cyber stalker/bully and victim to be thousands of miles apart (Jaishankar, 2011).

Like with traditional stalking and bullying, the motive is usually not sexual obsession. The motive usually involves hostility and aggression because of power and control issues. Very commonly, stalkers and bullies have mental disorders including paranoia or delusions. The internet makes these power and control issues even easier to unleash upon the victim. The internet's anonymity and global reach means the stalker can have even more power and control over the victim's life than normal stalkers. One major difference between the traditional stalker and the cyber stalker is that the cyber stalker is much more likely to choose their victim at random. The majority of traditional stalkers had a prior relationship with the victim, but up to 50% of cyber stalking cases involve no prior relationship. In one study, 41% of cyber bullying victims didn't even know who the

offender was. While many people in law enforcement view cyber stalking cases as relatively harmless, incidents have been known to escalate to violence. Even with the modern media exposure, many parents are not concerned about cyber bullying. 56% said they are not concerned about their child being bullied electronically, and 19% said they believe electronic bullying is rare (Jaishankar, 2011).

Laws designed to protect people from cybercrime are generally targeted at e-commerce, so cyber stalking/bullying has received little attention from lawmakers. What few laws do exist are usually only designed to protect certain groups. For instance, in the United States the Megan Meier Cyber Bullying Prevention Act protects people under 18 from cyber bullying and the Violence Against Women Act protects women from cyber stalking, but these laws only protect some people in some situations. Many other laws concerning cyber bullying are in place not to protect potential victims, but to protect the corporations running the online services from prosecution in cases of cyber bullying. Because of this lack of attention paid to cyber stalking and cyber bullying by legislators and police, the chance of being prosecuted is extremely low and the recidivism rate for cyber stalking and cyber bullying is around 50% (Jaishankar, 2011).

The courts have also consistently ruled that cyber bullies and stalkers are often within their first amendment rights. In one case, a male wrote a graphic and vivid story about the rape and torture of a female classmate and told his friends that he was going to carry out the rape. The court ruled that there was no violation of the law because rape over the internet was impossible. In another case, a boy made a mock obituary website for fellow students at his high school, and created polls for which student should be the next to die. The court ruled that he wasn't threatening anyone. Another high school

student created a web page accusing his assistant principal of being an alcoholic Nazi, and the court ruled that his cyber bullying caused no disruption to the learning environment. All of these cases are graphic illustrations of the difficulty in punishing cyber bullies and cyber stalkers (Jaishankar, 2011).

Cyber Fraud

Cyber fraud can take many forms, from the classic Nigerian Prince Scam (also known as the 419 scam, because the laws prohibiting the scam are in section 419 of the Nigerian penal code) to identity theft, credit card fraud, and insider trading (Denny, 2010). The various forms of fraud all have the ultimate purpose of extracting money or something else of value from an unwilling victim, and the more prevalent forms of fraud are very monetarily lucrative for the perpetrator. Cyberfraud was estimated to cost e-commerce websites 2.6 billion dollars in 2004 (Hoar, 2005), and identity theft was estimated to cost Americans 51 billion dollars in 2008 (Nykodym, et. al., 2010). Cyber fraud is getting more and more popular every year, thanks to low arrest and conviction rates and a high return for the perpetrator (Nykodym, et. al., 2010). Credit card fraud has become so popular that stolen credit card numbers are the unofficial currency of many hacker groups (Verton, 2002).

The fastest growing form of cyber fraud is identity theft, in which one person takes the identity of another and proceeds to use that identity to gain money through credit cards, loans, or some other monetary process requiring identification documents (Hoar, 2005). Fraudsters have been known to rent hotel rooms, break into wireless networks within range of that hotel room, and then gather information on potential victims through that wireless network. That information is then used to apply for credit

cards, which are used to purchase luxury goods which can be kept or sold for cash (Winmill, Metcalf, & Band, 2010). In 2009, one in twenty Americans was the victim of some level of identity theft (Hoar, 2005). Numerous laws have been passed to try and stop identity theft, such as the Identity Theft and Assumption Deterrence Act of 1998 and the Identity Theft Penalty Enhancement Act of 2004, but identity thieves are still rarely found and prosecuted (Winmill, Metcalf, & Band, 2010).

One of the more popular methods of fraud over the internet is phishing. In a phishing attack, a scammer will send out huge numbers of official looking e-mails that are designed to elicit personal information from the targets. This personal information can include passwords, banking information, social security numbers, account ID numbers, ATM PINs, and credit card information (Nykodym, et. al., 2010). There are other versions of this scam including spear phishing where a phishing attack is targeted at one individual, and pharming in which a piece of malware is used instead of an e-mail to direct people to a fake website. Law Enforcement has had trouble finding and prosecuting phishers, but there was a recent FBI operation code named "Operation Phish Phry" that resulted in the arrest of over 50 people accused of phishing over two million dollars from victims (Nykodym, et. al., 2010).

Over five million US citizens are victimized by phishing scams every year (Nykodym, et. al., 2010). About 19 percent of those who have received a phishing e-mail admit to having clicked the link contained within, and 3 percent say they gave the phisher financial or personal information. In 2005, one organization reported that they had evidence of over 15,000 unique phishing e-mails on the internet (Hoar, 2005). The most successful phishing e-mails are designed to target people with assets, so most of these e-

mails claim to be from financial institutions such as banks, credit card companies, or online financial organizations like Paypal. The scammer will use a web address that is similar to the address of the company they are pretending to be. For example, scammers may create a website that looks exactly like Paypal.com, but the address will be Paypa1.com. This means the victim would have to pay much more attention to the website their browser is viewing before they would realize the website is not actually Paypal (Nykodym, et. al., 2010).

Child Pornographers and Child Predators

On the internet, there are two kinds of predators that prey on children. There are the passive pedophiles that merely look at pictures or videos of child sexual acts, and there are active pedophiles that use the internet to find and recruit victims. Both are using the internet to commit the crime of taking advantage of children who are too young to consent to sexual acts. The number of passive pedophiles who download child pornography is very difficult to determine. It is very rare for a child pornographer to be reported to the police, and this reporting usually follows the discovery of the child pornography by friends, family members, or people the offender has entrusted their computer to (such as repair technicians). It is unknown how many other people have child pornography and are never caught. It is known that it is much easier to obtain child pornography on the internet than it would be anywhere else, because the anonymous nature of the internet makes this type of deviant behavior easier to engage in (Jaishankar, 2011).

The estimates that do exist say that child pornography is about a three billion dollar a year industry, gets searched for about 116,000 times a day on peer-to-peer file

sharing websites, and is featured on more than 100,000 websites around the world (Hoar, 2005). These estimates are conservative, and many groups put the numbers orders of magnitude higher. To be held liable for a criminal offense under US law, offenders do not even have to manually download any child pornography onto their computer's hard drive. Merely viewing child pornography online and having that image saved in their computer's temporary internet files (called a "cache") can be enough to charge an offender with possession of child pornography (Balkin, 2007). Law Enforcement has been able to focus on child pornography despite the difficulties in investigating it, because of the large public outcry and demand for enforcement from citizens worldwide. Recently, Operation Cathedral investigated a child pornography group called The Wonderland Club and arrested over 100 people that were involved across 14 countries in Europe, Australia, and North America (Jaishankar, 2011).

Active child predators are easier to find and prosecute than the passive child predators. In part, this is because they are soliciting young people for sexual encounters, and those young people often contact the police (or other authorities) to report this. About one in five juveniles on the internet are solicited for sex at some point (Hoar, 2005). While there are many media stereotypes of the way predators lure children into sexual relationships, many of these have been shown to be myths. Internet predators very rarely deceive their potential victims about the fact that they are much older and looking for a sexual relationship. They are up front about the fact that they are much older (usually males) looking for a sexual relationship from the youth. The victims in almost all cases were not abducted or otherwise physically abused at any time, but agreed to meet the predator for sexual purposes. This is not to say that child predators aren't criminals or

that their crimes should be excused, but the way the crime happens is often misunderstood and misrepresented by the media (Wolak, Finkelhor, & Mitchell, 2004).

Cyber Terrorism and Cyber Warfare

In 1999, President Bill Clinton said "Terrorist and outlaw states are extending the world's field of battle, from physical space to cyberspace, from our earth's vast bodies of water to the complex workings of our own human bodies" (O'Neil, 2006, p.233). Cyber terrorism has only become more popular since that was originally spoken, and over 4,000 websites for terrorism are known to currently exist on the internet with an unknown number of others that have not been detected (Hoar, 2005). Most of these websites and most terrorist activity on the internet is for the purposes of communication and training. Terrorists use the internet to plan and coordinate crimes, but there are increasing opportunities to use the internet in more directly destructive ways. In America especially, there is a growing amount of infrastructure that is dependent on the internet. The power grid, banking, health care, manufacturing, air traffic control, communications of all kinds, and many other systems that society depends on are vulnerable to attack through the internet directly. Terrorists can disable or destroy many of the components that are part of these networked systems that first world economies and societies depend on (Balkin, et. al., 2007).

Terrorists can use many of the techniques described in this paper to accomplish these ends. There have already been documented cases of terrorist activity against US military and civilian targets. During the Kosovo conflict, a Serb hacker group was able to hack into and delete all the information from a Navy computer (O'Neil, 2006). Another common tactic is for terrorist organizations to use stolen credit cards to fund their non-

cyber activities around the world (Winmill, Metcalf, & Band, 2010). Terrorists often use a process called steganography to hide data within other data. This process can hide terrorist plans or instructions within other data such as an image file or music file, making it difficult to trace who the intended recipient is (Balkin, et. al., 2007).

Cyber terrorism does not require extensive skills or training. In 2004, staffers for Senators Orrin Hatch and Bill Frist were caught stealing computer files from opposition party servers. More than 4,700 government documents were taken and saved on the staffers' computers. Neither of the staffers had any appreciable hacking knowledge. Luckily in this case, it was Americans who were able to steal these sensitive government documents and not terrorists (Balkin, et. al., 2007). In the UK, a 42 year old man named Gary McKinnon gained access to over 97 US government computer systems, including Army, Navy, and NASA computer systems. One of the reasons the US fought so hard to extradite McKinnon from the UK to the US is that they were embarrassed about how easy it was for him to hack into those systems. McKinnon had no terrorist motivations. He was a conspiracy theorist looking for evidence of UFOs. If he had been a terrorist, there is no telling how much damage he could have done (Arnell & Reid, 2009). If amateurs find it easy to break into US government computer systems, a legitimate hacker with terrorist motives would be easily able to cripple the United States Government. There is already evidence of terrorists recruiting experienced hackers for the purposes of cyber attacks (Mitnick & Simon, 2006).

Cyber warfare would look very similar to cyber terrorism, but would be committed by a national government instead of a terrorist organization. Foreign governments already have large groups of hackers working for them in an attempt to

prepare the battlefield for potential future wars (Verton, 2002). The US government is creating groups of hackers tasked with protecting the US government's computer systems from foreign attack (O'Neil, 2006). It is believed by many that hackers are the best option for defending computer systems from other hackers. This job will be extremely difficult, because there are numerous examples of foreign nations attacking the computer systems of the US and its allies. China's Operation Aurora targeted 34 Western companies, many of which are government contractors. Operation Aurora followed other Chinese cyber-attacks (nicknamed "Titan Rain" and "Ghostnet") which also targeted corporate and government computer systems around the world. They also used Denial Of Service (DOS) attacks against the websites of Chinese dissidents hosted in the United States. (Gutmann, 2010). NATO computer systems have been attacked and the US Navy was the victim of three days worth of intense attacks in 1998 that seemed to originate from one large source (such as a national government) rather than many distributed sources (such as non-government hackers) (Verton, 2002).

Hacker Groups

Hackers have been forming groups since the very earliest days of computers. The original hackers at MIT started as a group called the Tech Model Railroad Club, and sharing information within the group became one of the central principles of the hacker ethic (Levy, 2010). Early hackers in California joined groups such as the Homebrew Computer Club to share their latest creations with others. These groups usually formed using advertisements in early newsletters such as Technical Assistance Program (TAP) and Youth International Party Line (YIPL) (Thomas, 2002). In the 1990's, more groups would emerge such as the Cult of the Dead Cow, which was the first group to take media

seriously and use it to their advantage. A group called L0pht arose which was able to create their own networks for their members to break into, making hacking legal and safe. The information gained from these hacking sessions was then used to create hacking software such as l0phtcrack, which is used to break into Windows systems. Other groups such as the Legion of Doom and Masters of Deception have also been famous hacker groups during this period (Thomas, 2002). Hacker groups are not solely an American phenomenon. China has the Green Army and the Red Hacker Alliance (Gutmann, 2010), Germany has the Chaos Computer Club (Mitnick & Simon, 2010), and Russia has numerous organized crime groups that employ hackers to do the crime network's bidding (O'Neil, 2006).

The reasoning behind hackers joining together in groups is varied. For many, it is about sharing information (Verton, 2002). It is especially important for hackers to share what are known as "zero day" exploits. These are vulnerabilities in software that have just been discovered and aren't known outside of a select group of people (usually the hacker that discovered the exploit and his or her friends) (Mitnick & Simon, 2006). Hackers also group together so they have help for hacks that require the participation or expertise of a wide variety of people (Mitnick & Simon, 2006). It also provides the members with a healthy sense of competition with their peers, which can cause them to improve their hacking ability in an attempt to win an informal competition with their fellow group members (Thomas, 2002). In very large groups, there is strength in numbers. If thousands of people band together to break a cyber law, the police cannot find and arrest them all. In addition, large groups can make large, tedious projects such as sifting through huge amounts of data a much easier task (Olson, 2012).

Most of these groups are not well defined. They are mostly loose knit, with members from numerous places around the world. They are informal groups with membership being ambiguous at times (Verton, 2002). Hacker reputation is based in part on which groups they are affiliated with, but it is also heavily based on the information they choose to share with those groups. A hacker who has the ability to find zero day exploits and shares those with their group will gain reputation quickly. A hacker who breaks into a system that nobody else has broken into yet and shares evidence of that conquest will also gain reputation quickly. In many cases, this information sharing is enough to prove the hackers' claims, but not enough to allow another hacker to recreate the hack. Hackers will often keep the specifics of how they broke into a system a secret, and will refuse to share stolen or broken passwords or specific bugs that they utilized (Thomas, 2002).

Hackers often have informal meetings as well. Many hacker gatherings have happened over the years, including SummerCon, PumpCon, HoHoCon, and HOPE. One of the largest of these gatherings is DefCon, an annual meeting for hackers held over a three day period in Las Vegas, Nevada. It brings together hackers of all kinds, security experts, law enforcement, and other computer specialists to discuss the latest trends in computer security. One of the highlights of the convention is the "Spot the Fed" competition, where hackers are invited to try and find an undercover FBI agent in the crowd (of which there are usually many) and bring them up on stage (Thomas, 2002). Recently, they have added contests for hackers to prove their skills and compete against one another in an organized environment (Verton, 2002).

There are downsides to joining a hacking group, as well. As the famous hacker Kevin Mitnick said, "when your friends are people who are breaking the law, you're naïve if you expect loyalty" (Mitnick & Simon, 2011, p.205). Hackers can and will inform on each other in order to lessen their own sentences. The more people that are in a group and the more people who know of your exploits, the more likely it is that one of those people will give evidence to a law enforcement agency. In some cases, police will arrest people in a hacker group and demand that they inform on their "higher-ups." It can be difficult or impossible to make law enforcement realize that in many groups, there is no such thing as a "higher-up." In many cases, the group is run entirely on an egalitarian basis, with no leaders (Thomas, 2002). As an added downside to joining a hacking group, if police can't make hackers inform on other members of the group or have enough evidence to convict the group members for computer crimes already, they can also add in criminal charges for conspiracy (Thomas, 2002).

The most famous hacker group of the modern era is Anonymous. Anonymous arose out of the users of the popular website 4chan.org. Many in Anonymous would contend that Anonymous isn't a group at all, let alone a hacker group. They would say that Anonymous is a movement that people are free to associate themselves with or not. Anonymous has no leaders and no members. It has only those people who agree to work together to accomplish a specific goal at a specific point in time. When that goal is accomplished, the group disbands until another goal is identified, at which time a new group forms to accomplish that goal which may or may not contain some of the same people from the first group. They take pride in the fact that they have no leaders and nobody giving orders. One person will suggest an operation and if enough people agree,

the operation is carried out. If the person's suggestion doesn't attract enough people to go forward, it is dropped and ignored (Olson, 2012).

Anonymous is known for mass pranks that they call raids. The first major raid by Anonymous was a prank on a website running a game called Habbo Hotel where Anonymous members created avatars and denied the website's legitimate users access to popular areas of the game. Other raids involved antics such as posting pornography or extremely graphic content on family websites. They first attracted serious law enforcement attention after Denial of Service attacks against the Church of Scientology in 2008. The horde of Anonymous participants used a computer program to flood the Scientology website with junk messages causing the website to crash. In 2010, they took down Paypal, Mastercard, and Visa websites because those companies stopped accepting donations for Wikileaks, which had published large amounts of classified US government information previously in 2010. This incident caused a company called HBGary to start investigating Anonymous, and this company later contacted US government officials saying they could help in the investigation and arrest of Anonymous leaders. In 2011, Anonymous found out about this and hacked into HBGary's servers, and released thousands of e-mails and classified corporate documents. Anonymous also took over the company Twitter account and web site. Later in 2011, Anonymous attacked The Westboro Baptist Church, Sony, and the FBI (Olson, 2012).

One thing that sets Anonymous apart from other hacker groups is that there is little or no technical skill required to participate in many of Anonymous's activities. Most hacker groups will only accept members with expertise in computer coding and security, but Anonymous being set up the way it is with no hierarchy and no real membership

means there are no requirements to participate in their group attacks. For instance, if a person wants to participate in an Anonymous Denial of Service attack, they must only know how to access the Anonymous IRC chat room, download a simple program, input the address of the server the group is targeting, and click a button. Only a very small portion of the group are actually hackers with exceptional technical abilities (Olson, 2012).

The media and law enforcement has a very inaccurate view of what Anonymous actually is. They are described as terrorists and Nazis. They are seen as a cohesive group with a hivemind that attacks for their own personal gain or because of childish pettiness. The truth is nowhere near as clear as those groups make it out to be. In reality, Anonymous is different things at different times, because the group is constantly evolving and changing. Anonymous is a label that anyone can claim, so people committing a crime under the name of Anonymous today and people attacking a government website tomorrow may both call themselves Anonymous when in reality no individuals participated in both events. The group has no sense of right and wrong. If someone posts an idea for a prank or a mission that others think is funny or interesting, they will work together to complete it regardless of whether that goal is legal or illegal, moral or immoral (Olson, 2012).

Hacker groups do not spend all their time on malicious pranks and internet crimes. They have also been known to work very hard improving the world in many significant ways. Falun Gong hackers created a program called Dynaweb which allows Chinese internet users to bypass the government internet censorship that prevents Chinese citizens from accessing many parts of the World Wide Web (Gutmann, 201).

The Genocide2600 group would frequently find and bait pedophiles and child pornographers online, and then turn over that evidence to the police (Verton, 2002). The group L0pht found numerous bugs in the Microsoft Windows operating system and reported them directly to Microsoft in the hopes that Microsoft would fix those problems (Thomas, 2002). There are many hacker groups that work towards political and social goals as well. For instance, some members of Anonymous worked very hard to take down the Syrian government's websites and internet services during the Syrian Civil War (Olson, 2012). Other hacker groups worked hard to publicize the violation of Kevin Mitnick's civil liberties during his trial and incarceration in the late 1990s (Thomas, 2002).

Hackers

There are many stereotypes about who hackers are. The media portrays hackers as teenage males that are extremely intelligent, socially awkward, middle class, either very skinny or very fat, suffer from acne, wear glasses, have very few friends, etc. There is very little information in the literature that confirms or disproves any of these stereotypes. In many cases, it is unclear whether the claims made by authors are from actual studies or if the author is just repeating the stereotype. In addition, the hacker community has changed drastically in the preceding decades and some aspects of the stereotypical hacker profile may have been true at one point but are no longer reflective of reality.

There is ample evidence that hackers begin their computer crime careers at a very young age. Bill Gates says his most prolific years of hacking were 13 to 16 (Levy, 2010). Other hackers started as early as 10 or 12 (Verton, 2002). The youngest person ever convicted of hacking in Federal Court was just 16 years old (Mitnick & Simon, 2006).

The reason hackers may start so young is because it is easier to rewire the brain at a young age. Some theorize that learning to be a hacker is similar to learning a new language, and that when a person is still developing, their brain has an easier time learning an entirely new way of thinking (Mitnick & Simon, 2006). Whatever the reason for the increased hacking activity of youth, hackers have traditionally not cared about other hackers' ages. The only thing hackers judge others on is their hacking ability (Levy, 2010). Some have attempted to find the average age of different types of computer criminals. One study of hackers in Israel shows that the average age was 24. In another study of software and media pirates, the youngest age group (18-29) was by far the largest of all age categories (Jaishankar, 2011). The average age of Anonymous hackers that have been identified and arrested was 24 (Olson, 2012). Most of the information available about the age of computer criminals is anecdotal, and it is hard to establish what impact the "newness" of the technology involved has on the age of computer offenders. There is no research that actually compares the average age of computer criminals to the average age of any other crime category.

There are similar issues when examining the gender of computer criminals. In the early days of computers, there were no female hackers. There were female programmers, but none lived it as a lifestyle the way the famous early hackers did. In fact, most women expressed an extreme distaste for what they viewed as the "man's world" of computers. This male dominated culture is also seen in the language used by hackers, where they commonly use words like "penetrate," "rape," and "ravage" the other persons' computer, which is often portrayed as feminine (Thomas, 2002). This gender imbalance in the world of computers was partly responsible for the incredibly high rate of divorce among early

computer hackers. Wives lost their husbands to computers (Levy, 2010). Numerous studies have shown that even today, the vast majority of computer criminals are men. In one study of internet predators, the offenders were 99% male (Wolak, Finkelhor, & Mitchell, 2004). In a study of Isreali hackers, there were 54 males and only three females (Jaishankar, 2011). A study of Korean teenagers showed that males were much more likely to become software pirates than females, but part of this effect was due to the fact that boys had much more opportunity to pirate because they used computers more often (Moon, et. al., 2012). The vast majority of Anonymous members are single males. In fact, there is a popular catchphrase among Anonymous members that "there are no girls on the internet" (Olson, 2012, p. 55).

This male dominated culture seems to be changing. Already there is evidence that some computer crimes are fairly evenly split between males and females, such as piracy and Nigerian Prince scams (419 scams). There is still evidence that they may still be differences in the way the different genders take part in these crimes, however (Jaishankar, 2011). Hackers of all kinds are becoming increasingly female, although there is still the perception that men still vastly outnumber women. A female recently won a major hacking competition at DEFCON (Verton, 2002). Kevin Mitnick sees more and more female social engineers, who have an advantage over their male counterparts because they can often use their sexuality as a social engineering tool to persuade male targets to give up information (Mitnick & Simon, 2002).

This trend towards women hackers may be less straightforward than it may seem at first glance. The anonymity of the internet allows people to claim to be female when they are actually male. These false claims are a well known internet phenomenon, and

can skew the perceived ratio of male to female on the internet. Along similar lines, there are a high number of LGBT and transgender people in groups like Anonymous. In one large Anonymous chat room, about one third of all participants identified as LGBT. An unknown (but likely high) number of female hackers are likely to be male to female transgendered individuals. Any study of hackers that includes an investigation into gender must make accommodations for this higher than normal instance of transgender individuals if the researcher wishes to make an accurate assessment (Olson, 2012).

Race is another issue that is hard to measure, especially with the anonymity of the internet. African Americans and Hispanics are vastly over represented among software pirates and child porn viewers (Jaishankar, 2011) but these are the computer crimes that are among the least dependant on technical skill and have the least to do with traditional hacker culture. The overwhelming majority of the technically proficient hackers are white, and despite the fact that the hacker ethic claims that things like race shouldn't matter, there is rampant racism among many hacker communities. Hacker communities are usually made up of young males, which facilitates an environment conducive to frequent expressions of racism. If confronted with accusations of racism, these young males will usually claim it was a joke, and that they really don't care about race (Thomas, 2002).

Because the original hackers were at universities such as MIT, hackers are stereotyped as being very educated. This may be becoming less and less accurate over time. In one sample of software pirates, a plurality of pirates had less than a high school diploma and the smallest group was college graduates. In another sample of hackers in Israel, 74% had the equivalent of a high school diploma. In a study of child porn users,

over 60% had a college degree (Jaishankar, 2011). It is not unheard of to find hackers who have skipped three grades during their education (Verton, 2002). This may be one of the hardest descriptive statistics to accurately assess for hackers. The anonymity of the internet combined with the overwhelming youth of computer criminals makes it hard to determine if their education levels are low because they failed/dropped out of high school or whether they are just young and haven't graduated yet.

Income is another variable that is probably highly dependent on age. In one sample, internet piracy was remarkably even among income groups. Among a sample of Israeli hackers, 74% had above average household incomes. Cyber stalkers and cyber predators are also much more likely to have middle or upper class incomes, but child porn viewers were much more likely to have lower class incomes (Jaishankar, 2011). The overall pattern seems to be similar to pattern seen with race and education: the criminals who commit computer crimes that require a low level of technical skill are different from the criminals who commit computer crimes that require more technical skill. There is one piece of data that shows why computer criminals may have higher incomes than other criminals. Around 90% of all cyber attacks on businesses are internal attacks by employees (Jamil & Khan, 2011). This means a large percentage of all cyber criminals are going to be individuals with a job in a company that allows them the access to computer networks needed to commit these crimes.

There are a few other measurable statistics by which computer criminals have been assessed. For instance, Israeli hackers are overwhelmingly secular (83%) and unmarried (78%), cyber stalkers are very likely to have a prior criminal record, the majority of child porn viewers are unmarried (63.3%), and the vast majority of cyber

predators suffered from internet addiction (Jaishankar, 2011). It is apparent that no researcher has previously examined any of these simple descriptive statistics in an attempt to determine whether stereotypes about hackers are accurate, or to determine if computer criminals are different from other criminals.

There are other, not so easy to measure stereotypes and common beliefs about who hackers are, what motivates them, how they act, and what they do. For instance, there is a commonly held belief that hackers are anti-social loners with poor social skills. This belief has been around since the early days of hacking, prompting one observer to remark "It was sort of necessary for these people to be extremely brilliant and in some sense, handicapped socially so that they would just kind of concentrate on this one thing" (Levy, 2010, p.133). Some early hackers stated they were specifically denying themselves fun in order to spend more time focusing on their work. It was understood that computers would take up so much of a real hacker's time that they would have no room for a social life. It was such a common belief among hackers and non-hackers alike that even famous psychologist Philip Zimbardo commented in 1980 that hackers were "antisocial losers who turned to computers to avoid human contact" (Levy, 2010, p.472).

Kevin Mitnick fit this mold. He was in the top 1 percentile in math and spelling, and he and his friends were "socially inept and uncool" (Mitnick & Simon, 2011, p. 10). Today, this tradition is changing. Hackers are still very private people (as a general rule) but that does not prevent them from being social and active. There is ample anecdotal evidence that today's hackers are more likely to spend time doing "normal" things, like going to parties, playing sports, and spending time with non-hacker friends. Some young hackers play on the soccer team, another was a varsity wrestler. They are no longer the

stereotypical geeks who only have online friends, stay in their rooms all day, refuse to participate in physical activity, and are socially awkward and shy. Computers have become such a normal part of everyday life that average people are becoming hackers (Verton, 2002).

Hackers are also believed to be incredibly curious. They are described as having a compulsion to take things apart to see how they work, and it is this curiosity (especially with electronic or digital things) that drives them to become hackers in the first place (O'Neil, 2006). This curiosity drives their thirst for information, which drives a strong and intense desire to know secrets. This knowledge of secrets has become one of the most important factors in the status that a hacker has in the community. If they know secrets, then they are considered elite. This curiosity and desire to not only know secrets but to publish them for the world to see is a threat to those who have a tendency to keep secrets such as governments and corporations, which is why these groups work so hard to demonize hackers (Thomas, 2002).

Hackers have been portrayed by the media and perceived by the public in many different ways. This labeling is usually made up of name calling and shaming in order to separate the Hacker as an "other" and an enemy (Halbert, 1997). They are "evil deviants" (Dudek & Johnson, 2011, p. 185) and "villains" (Nissenbaum, 2002, p. 52). They are often even compared to violent criminals, with hacker groups sometimes portrayed as being involved in a "gang war" or hackers being called "serial hackers" with all the connotation that is usually accompanied by the term "serial" in criminal justice (Thomas, 2002). This view is becoming less pervasive over time. More and more, people are

beginning to see computer criminals as different. They are starting to be seen as less evil and less of an "other" as the world becomes more computer dependant.

Hackers themselves claim that they are "positive deviants" and that their actions are an important part of any computing society (Jaishankar, 2011). They realize that what they do is against the rules, but they see their crimes as beneficial to the internet and the world. Many hackers would say that they improve the world by shaking faith in the system. These hackers see a world in which the authority figures are the bad guys and thus since the hackers fight against these authority figures, they must be the good guys. To them, computer crime is about rebellion (Thomas, 2002).

Outsiders have compared hackers to many different groups. Some have compared them to artists, with computers being just another medium of expression. Digital data is to hackers what paint is to artists or instruments are to musicians (Nikitina, 2012). Coleman (2011) sees hackers as the modern embodiment of the classic liberal. They are obsessed with notions such as freedom of expression, privacy, and meritocracy to the point of breaking any laws that get in the way of those principles. Many people view hackers as magicians, because they can perform tricks on a computer that are similar to a magician's tricks on a stage (Thomas, 2002). Similarly, some people describe hackers as tricksters; not in the "magician" sense but in the ancient sense of a deviant supernatural being who plays tricks on humanity (Nikitina, 2012). In this view, hackers are similar to the ancient Norse god Loki, famous for pulling pranks on humanity and causing chaos for his own amusement.

One of the more interesting views on how hackers fit into the world comes from Wark (2004) who claims that the separation between the "haves" and the "have nots" has

shifted for only the second time in recorded history. For the first major period in human history, the powerful were the people with land and the peasants were the people who didn't have land. The peasants staged many revolts against the landed, powerful members of society. This differential power structure was finally overcome with the rise of capitalism, when the power ceased to be vested in land and became vested in capital. At that point, the powerful had money and those without money had no power. Again, there were many uprisings and revolts by the poor because of this capitalist system. Wark believes that the modern world is in the process of shifting again to a situation in which the powerful aren't the ones with the money, but the ones with the information. The weak in society will be those without the access to information. Hackers, in this view, are the uprising of those without information against those who are hoarding information for themselves (governments and corporations). According to this view, hackers are freedom fighters attempting to even the playing field for humanity with regards to information. Digital communists, so to speak.

Notorious hacker Kevin Mitnick has a different take on how hackers fit into modern life. He quotes other hackers in saying that hacking is more like a religion than a hobby or an occupation (Mitnick & Simon, 2006). When he hacks, he says he feels like an explorer, going places for the thrill of being in a place he wasn't supposed to be. He bypasses security put in place by engineers with years of experience for the simple joy of exploring the system that they were trying to keep secret (Mitnick & Simon, 2011).

Mitnick also warns that many of the people on both sides of the issue are building hackers up to be something they're not, and this can be dangerous. He takes the comparison of hackers to magicians and points out that in the middle ages, magicians had

myths built up around them so much that people believed they were all powerful, in league with the devil, and thus must be killed on sight. He sees a similar process of myth building happening with hackers. They are being so glorified by both the people who think they are a beneficial group and by those who think they are a menace that the general public has a completely distorted view of who they are and what they can actually do. As evidence, he discusses the incident he experienced in a court room when a prosecutor claimed that Mitnick could whistle tones into a phone and cause a nuclear missile launch. This would be technically impossible, but it was taken seriously because of the myth building about hackers in general and about Mitnick himself (Mitnick & Simon, 2011).

Hackers are believed to be a certain type of person despite little modern evidence that they actually reflect the stereotypes of a "hacker". There is ample evidence that the original computer criminals conformed to the stereotypes that they helped create. They were overwhelmingly educated white males with social interaction issues. They were computer criminals because of a strict code of ethics that was developed around computing in the 1960s. Computing has changed drastically in the intervening decades, however. Computers are now commonplace and are used by far more people than just university students and business people. This shift in the demographics of computer users may have also affected who hackers are, where they come from, and why they do what they do. The commonly believed stereotypes may no longer be an accurate representation of hackers.

III. METHODS

This work is an attempt to discover what makes hackers different from other criminals. It will quantitatively examine what makes those who commit crimes on computers different from those who commit other crimes. Each group will be identified within a large secondary data sample and the two groups will be compared statistically to determine if there are any significant differences between them. A subsequent set of analyses will examine how subsets of computer criminals differ from each other.

Sample

The sample that will be used for the statistical analysis in this study is the Survey of Inmates in State and Federal Correctional Facilities, 2004. It is a dataset created with data from a survey given to Federal and state inmates by the United States Department of Justice and the Bureau of Justice Statistics. The data was gathered between October 2003 and May 2004. The dataset is available through the National Archive of Criminal Justice Data and the Inter-university Consortium for Political and Social Research (ICPSR). Previous versions of the survey were given in 1974, 1979, 1986, 1991, and 1997.

A two stage cluster sample was used to generate the sample. In the first stage, a population of 1,585 state prisons and 148 Federal prisons was identified, and a sample of 231 male state prisons, 70 female state prisons, and 40 Federal prisons was selected using a systematic random sampling method. 225 male state prisons, 62 female state prisons, and 39 Federal prisons agreed to cooperate. Prisons which reported medical, mental health, and geriatric care specialties were given higher weighting in order to guarantee their representation in the final sample.

From these facilities, a computerized stratified sampling technique was used to draw a state prison sample of 13,098 male inmates and 3,054 female inmates and a Federal prison sample of 3,347 males and 1,009 females. In the Federal sample, non-drug offenders were given higher weights due to the high percentage of drug offenders in Federal prisons. Computer assisted personal interviewing techniques were used in which an interviewer asks questions that are prompted by the computer and the interviewer inputs the responses back into the computer which can prompt follow-up questions based on the answer given. All inmates were informed that participation was voluntary both in writing and verbally by the interviewer. The overall response rate for state inmates was 89.1 percent and the response rate for Federal inmates was 84.6 percent.

There are many benefits to using secondary data. The most obvious is the cost savings. This dataset and many more are available free of charge from the ICPSR. Researchers of all kinds are able to use the datasets hosted there at no charge, significantly lowering the monetary costs of research. In addition, secondary research reduces the time needed to complete the research. In this case, it would take months or years to compile the information needed for statistical analysis but only a matter of minutes to download and begin to examine the information from the ICPSR archive.

There are also negatives to using secondary data. Often, it is unclear exactly how the data was gathered. Precise question wording is an important factor in measuring constructs as accurately as possible, and this question wording may not be clear or may not be measuring the construct exactly as the researcher using the secondary data would like. Because of the information available about the data collection methods and based on

the previous research using this dataset, the researcher is confident that the variables in this dataset are valid measures of the constructs the study is attempting to measure.

Variables and Hypotheses

Age. Variable V0017 is the measure for age. The question was asked using the wording "How old are you?" and valid responses range from 1 to 96. A value of 97 indicates an "I don't know" answer and a value of 98 indicates a "Refused to answer" response. A value of 99 indicates a blank response. This variable is continuous.

The age variable is important to this research because the common belief is that hackers are very young. Because computer technology is relatively new, it is the youth of America that are the most familiar with it. There is also the well known age/crime curve which shows that all crimes are overwhelmingly committed by young people, which may suggest that hackers are not younger than other criminals. The hypothesis for this research is that cyber criminals are significantly younger than other criminals.

Gender. Variable V0005 measures the sex of the respondent. There is no question wording listed in the dataset's codebook. There are only two possible responses; 1 indicates male, 2 indicates female. It is unclear how the researcher who collected the data dealt with any transgender or intersex individuals. This variable is a discrete variable.

Gender is an important variable because computer criminals are viewed as being overwhelmingly male. In the early days of computers, the overwhelming majority of computer users were males, but this trend may be changing in the twenty-first century. Computer users have become increasingly female since the male dominated 1960's and 1970's, but the common perception is that hackers are overwhelmingly male. The

hypothesis for this research is that computer criminals are more likely to be male than other criminals.

Race and Ethnicity. Variables V0018 and V0029 through V0034 measure the race and ethnicity of the respondent. The first of these questions measures whether the respondent is of Hispanic ethnicity, and asks "Are you of Spanish, Latino, or Hispanic origin?" The following questions measure the race of the respondent and are worded "Which of these categories describes your race?" The responses to the original question were split among six different variables, each one being a dummy variable measuring whether the respondent was of a certain race. The six racial categories are White, Black, American Indian/Alaskan Native, Asian, Hawaiian/Pacific Islander, and Other.

Race is an important factor in this research because computer criminals are perceived as being overwhelmingly white. In the early days of computers, computers were only available in universities and large corporations which were overwhelmingly white. This lower level of access to computers and to the economic power to purchase computers resulted in far fewer minorities becoming computer literate. This may have changed in more recent years with increased access and lower costs for computer equipment. The hypothesis for this research is that computer criminals are more likely to be white than other criminals.

Education. Variable V1740 measures the education level of the respondent. The questions is worded "Before your admission on [MOST RECENT ADMISSION DATE], what was the highest grade of school that you ever attended?" A variable value of 0 indicates no formal schooling or kindergarten only. A variable value of 1 through 12 indicates a response of first through twelfth grade. A value of 13 through 16 indicates

years of college education (Freshman, Sophomore, Junior, Senior). Values of 17 and 18 indicate attendance in grad school for one year and two years, respectively. A value of 19 indicates schooling in a foreign country in which the "grade" system does not translate. Values of 97, 98, and 99 indicate responses of don't know, refused to answer, and skipped. Variable 1741 asks "Did you complete that year?" Variable V1740 is a discrete variable.

Education is an important variable for this study because the popular perception is that computer criminals are more educated than other criminals. This belief stems from the early hackers being university students. Until relatively recently, computer users were either college students or had white collar jobs which require higher levels of education. It took some level of education to be able to learn how to use a computer and to have a job affluent enough to afford a home computer system. This correlation may be changing with the increased accessibility of modern personal computers. Due to the decreased costs and increase in availability and ease of use, computers are now owned by more than the educated members of American society. For this research, the hypothesis is that computer criminals are more likely to have higher levels of education than other criminals.

Analysis Plan

The investigation into the difference between computer criminals and other criminals used a logistic regression model to estimate whether any of the independent variables described above are significantly related to being a computer criminal. The researcher calculated a logistic regression equation with the computer crime variable as the dependant variable and the age, gender, race, and education variables as independent

variables in order to find out what relationship those variables have with each other. Regression is the process of modeling the mean of a dependent variable as a function of one or more independent variables. Logistic regression is one type of regression that is commonly used when the dependant variable for a regression equation is discrete. Logistic regression uses maximum likelihood estimation to approximate the log odds of the independent variables' effect on the dependant variable.

In this case, the dependant variable is V0856, which asks "Did you use a computer to commit or help you commit the [CONTROLLING OFFENSE]?" Responses include a 1 indicating a yes response, 2 indicating a no response, 7 indicating a don't know response, 8 indicating a refused to answer response, and 9 indicating a blank response. This variable was transformed by the researcher so that all responses other than 1 or 0 were designated as missing data and ignored. This transforms the variable to be a simple dichotomous variable with 1 indicating that the respondent admitted to computer crime and 0 indicating a "no" answer to the computer crime question.

After this main analysis, a series of further analyses was conducted using the identical set of independent variables, but changing the dependant variable to other variables that are designed to find out which subset of cyber crime the prisoner was incarcerated for committing. A total of eight dependant variables were substituted in addition to the main computer crime dependant variable. These eight variables were measures of which particular subset of computer crime the offender committed, and options consisted of stealing financial information, identity theft, illegal computer system access, obscene communication, copyright infringement, vandalism, forgery, and intellectual property theft.

Only offenders who had answered “yes” to the computer crime variable were given a chance to answer the questions regarding the precise type of computer crime they committed. Each variable is a simple dummy variable coded with a 1 for a positive response and a 0 for a negative response. It is hoped that an analysis of these variables will show how different subsets of computer criminals differ from each other. The hypotheses for the independent variables remain the same for all dependant variables.

IV. RESULTS

Descriptive Statistics

The first analysis conducted was a simple descriptive assessment of the data. When the data was obtained from ICPSR, it was already split between Federal Data and State Data. This separation of data was maintained throughout the analysis. The data in each sample (Federal and State) was sorted and then split by computer criminal and non-computer criminal. The means and standard deviations of each independent variable were calculated. The results are shown in Table 1.

Table 1. Descriptive Statistics

State Prison Sample	Age		Male		White		Education	
	Mean	Std. Dev	Mean	Std. Dev	Mean	Std. Dev	Mean	Std. Dev
Computer Criminals	34.19	9.68	0.43	0.49	0.57	0.49	13.10	2.64
Non-Computer criminals	35.07	9.72	0.74	0.43	0.44	0.49	10.87	2.29

Federal Prison Sample	Age		Male		White		Education	
	Mean	Std. Dev	Mean	Std. Dev	Mean	Std. Dev	Mean	Std. Dev
Computer Criminals	39.10	10.20	0.50	0.50	0.53	0.50	14.06	2.58
Non-Computer criminals	38.29	11.03	0.73	0.44	0.33	0.47	11.37	3.20

In the state prison sample, the mean age for computer criminals (34.19, std. dev 9.68) is almost one year lower than the mean age for other criminals (35.07, std. dev 9.72). In the Federal sample, the mean age of the computer criminal population (39.10, std. dev 10.20) is slightly higher than the mean age for other criminals (38.29, std. dev 11.03). Age is the only one of the four independent variables that shows a different

direction (higher for the computer criminals in one sample, lower for computer criminals in the other sample) for the Federal and state samples.

In the state prison sample, 43% of computer criminals were male compared with 74% of other criminals, and in the Federal sample 50% of computer criminals were male compared to 73% of the other criminals. This difference in percentage male is the opposite of the direction predicted by the hypothesis. The hypothesis predicted that computer criminals would have a higher percentage of males than females (compared to non-computer criminals) but this data shows that the computer criminals have a lower percentage of males to females than other criminals.

In the state prison sample, 57% of computer criminals reported being white (and non-Hispanic) compared to 44% of the non-computer criminals that are white (and non-Hispanic). The Federal sample showed 53% white (non-Hispanic) for the computer criminals and 33% white (non-Hispanic) for the other criminals. Both of these ratios are in the direction predicted by the hypothesis, meaning that the hypothesis predicts, and this data shows, that computer criminals have a higher percentage of white (non-Hispanic) prisoners than non-computer criminals.

The mean educations score for computer criminals in the state sample was 13.10 (std. dev. 2.64) compared to an average education score of 10.87 (std. dev. 2.29) for non-computer criminals. In the Federal sample, the mean education score for computer criminals was 14.06 (std. dev. 2.58) compared to a mean education score of 11.37 (std. dev. 3.20) for non-computer criminals. This ratio is in the direction predicted by the hypotheses, meaning that the hypothesis predicted, and this data shows, that computer criminals are more educated than other criminals.

Main Regression Analysis

The main analysis for this study consisted of a logistic regression equation with age, gender, race, and education as independent variables and computer crime as the dependant variable. Age was input as a continuous variable, gender was turned into a dummy variable with male as 1 and female as 0, race was turned into a dummy variable with white, non-Hispanics as 1 and other races and Hispanics as 0, and education was input as a continuous variable that closely corresponds to years of education (see analysis plan in Chapter 3 for a complete explanation of how the education variable was constructed).

Table 2. Main analysis

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.96*	0.01	-3.42	<0.01
White	1.29	0.23	1.38	0.16
Male	0.29*	0.05	-6.58	<0.01
Education	1.51*	0.05	10.86	<0.01
Constant	0.001*	<0.01	-12.16	<0.01

n = 4339 * = p<0.05

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.97*	0.01	-3.23	<0.01
White	1.53*	0.28	2.34	0.01
Male	0.44*	0.07	-4.64	<0.01
Education	1.35*	0.04	8.86	<0.01
Constant	0.01*	0.01	-9.13	<0.01

n = 1448 * = p<0.05

The results of the main regression analysis are shown in Table 2. In the state sample, the Z scores for age, male, and education are -3.42, -6.58, and 10.86, respectively. These values lie within the critical region, so we reject the null hypothesis and conclude at the 0.05 level of statistical probability that there is a difference between computer criminals and other criminals with respect to variables. The male variable is statistically significant, but in the opposite direction of that predicted by the hypothesis. While the hypothesis predicts that computer criminals will have a higher percentage of males compared to other criminals, the results show that computer criminals have a lower percentage of males compared to other criminals.

The odds ratio for the age variable is 0.96, which means that for every one year increase in age, the odds of being in state prison for a computer crime are reduced by roughly 4%. The odds ratio for the race variable is 1.29, but this variable was not statistically significant. The odds ratio for the gender variable was 0.29, which means that if the subject is a male, their odds of being in state prison for a computer crime are reduced by roughly 71%. The odds ratio for the education variable is 1.51, which means that for every one unit increase on the education scale, the odds of being in state prison for a computer crime rise by roughly 51%.

In the Federal sample, the Z scores for age, white, male, and education are -3.23, 2.34, -4.64, and 8.86, respectively. These values lie within the critical region, so we reject the null hypothesis and conclude at the 0.05 level of statistical probability that there is a difference between computer criminals and other criminals with respect to those variables. Like in the state sample, the male variable is statistically significant but in the opposite direction of that predicted by the hypothesis, meaning the percentage male for

computer criminals was predicted to be higher than the percentage male for other criminals, but the percentage male was actually found to be lower than the percentage male for other criminals.

The odds ratio for the age variable is 0.97, which means that for every one year increase in age, the odds of being in Federal prison for a computer crime drop by roughly 3%. The odds ratio for the race variable is 1.53, meaning that if the subject is white and non-Hispanic, their odds of being in Federal prison for computer crime increase by 53%. The odds ratio for the gender variable was 0.44, which means that if the subject is a male, their odds of being in Federal prison for a computer crime are reduced by roughly 56%. The odds ratio for the education variable is 1.35, which means that for every one unit increase on the education scale, the odds of being in Federal prison for a computer crime rise by roughly 35%.

Additional Analyses

In addition to the main analysis described above, the researcher performed a series of eight sub-analyses in which subsets of computer criminals were compared. If the respondent answered "yes" to the question "Did you use a computer to commit or help you commit the [CONTROLLING OFFENSE]?" then they were asked a series of follow-up questions designed to elicit which specific cybercrime law they were convicted of breaking. These questions were "Did you use the computer to gain unauthorized access to credit card number, bank accounts, or other financial information?", "… to steal the identity of another person?", "… to gain unauthorized access to a computer system?", "… to send lewd or obscene messages, communications, or images, while online or through e-mail?", "… to distribute computer programs which you did not have

permission to copy or distribute?", "… to vandalize or sabotage that computer or another computer?", "… to forge or alter documents?", and "… to steal intellectual property?"

These eight were turned into dummy variables with 1 indicating a positive response to these questions and a 0 indicating a negative response to these questions but a positive response to the computer crime question used in the main analysis. A series of eight logistic regressions were run with these eight dummy variables as dependant variables and the same independent variables as the main analysis. The results of these logistic regression equations are displayed in Tables 3 through 10.

The results may be biased because of incredibly small amounts of variation within the dependant variable. For these dummy variables, the number of positive responses ranged from 3 to 66 and the sample group was 135 in the state sample and 169 in the Federal sample. The very small amount of positive responses in a relatively small sample may have biased the results, so these results are presented only for completeness, and in the hope that further research will clarify the results presented.

There are many interesting results from these analyses. The odds ratios for age in both the Federal and state sample for the "Unauthorized Access to Financial Information" equation (Table 3) are 0.94, with a p value of 0.02. This means that for every one unit increase in age, the odds of being a cyber criminal convicted of unauthorized access to financial information is reduced by roughly 6%. This means that the computer criminals arrested for stealing financial data are younger than their other computer criminal counterparts. None of the other variables for this group were statistically significant.

Table 3. Unauthorized Access to Financial Information

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.94*	0.02	-2.22	0.02
White	1.07	0.43	0.17	0.86
Male	0.95	0.38	-0.12	0.90
Education	1.08	0.09	1.01	0.31
Constant	0.72	0.89	-0.26	0.79
	n=135		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.94*	0.02	-2.11	0.03
White	0.94	0.41	-0.13	0.89
Male	0.71	0.31	-0.77	0.44
Education	1.00	0.09	0.03	0.98
Constant	1.60	2.02	0.38	0.70
	n=169		* = p<0.05	

For the Identity Theft group (Table 4), there was a statistically significant odds ratio for age (0.94) but only for the state sample. This means that for a cyber criminal in state prison, for every one unit increase in age, their odds of being in prison for Identity Theft were reduced by roughly 6%. None of the independent variables for the Federal sample were significant.

Table 4. Identity Theft

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.94*	0.02	-2.41	0.01
White	1.11	0.45	0.27	0.78
Male	0.77	0.31	-0.61	0.53
Education	1.02	0.08	0.27	0.79
Constant	2.19	2.74	0.63	0.53
	n=135		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.97	0.02	-0.87	0.38
White	0.83	0.36	-0.41	0.67
Male	0.64	0.27	-1.02	0.30
Education	0.87	0.07	-1.43	0.15
Constant	3.30	4.15	0.95	0.34
	n=169		* = p<0.05	

For the Cyber Trespassing group (Table 5), the age variable was significant for both the state and Federal samples. For both samples, the odds ratio for Age was 0.92, which means that for every one unit increase in age, the odds of a cyber criminal being in prison for cyber trespassing was reduced by roughly 8%. None of the other variables in either sample were significant for the Cyber Trespassing group.

Table 5. Cyber Trespassing

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.92*	0.02	-2.72	<0.01
White	0.97	0.43	-0.05	0.96
Male	1.42	0.63	0.80	0.42
Education	1.17	0.11	1.65	0.09
Constant	0.39	0.54	-0.67	0.50
	n=135		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.92*	0.03	-2.32	0.02
White	0.65	0.34	-0.81	0.41
Male	0.87	0.45	-0.25	0.79
Education	1.22	0.13	1.80	0.07
Constant	0.14	0.22	-1.26	0.20
	n=169		* = p<0.05	

In the Obscene Communication group (Table 6), the Age variable in the state sample had a statistically significant odds ratio of 1.09. This means that for every one unit increase in age, the odds of a cyber criminal being in state prison for Obscene Communication rises by roughly 9%. In other words, those in state prison for obscene communication are older than other computer criminals. The Male variable was automatically omitted from the state sample statistical analysis by the computer program because of a collinearity issue. In the Federal sample, the Male variable has a statistically significant odds ratio of 4.24. This means that if a computer criminal in a Federal prison is male, they are 324% more likely to be imprisoned for obscene communication.

Table 6. Obscene Communication

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	1.09*	0.04	2.17	0.03
White	1.07	1.05	0.07	0.94
Male	omitted			
Education	1.22	0.19	1.26	0.20
Constant	<0.01*	0.00	-3.08	0.00
	n=59		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.96	0.02	-1.15	0.25
White	1.79	1.05	1.00	0.31
Male	4.24*	2.83	2.16	0.03
Education	1.11	0.12	0.99	0.32
Constant	0.01*	0.03	-2.29	0.02
	n=169		* = p<0.05	

In the Copyright Infringement group (Table 7), the statistically significant odds ratio for age in the Federal sample is 0.86. This means that for every one unit increase in age, the odds of being in Federal prison for copyright infringement decrease by roughly 14%. This was the most pronounced decrease in age for any of the eight groups. In the state sample, the education variable had a statistically significant odds ratio of 1.68. This means that for every one unit increase on the education scale, the odds of a computer criminal being in state prison for copyright violation increases by roughly 68%.

Table 7. Copyright Infringement

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.88	0.05	-1.92	0.06
White	0.74	0.65	-0.34	0.73
Male	1.02	0.89	0.03	0.97
Education	1.68*	0.32	2.68	<0.01
Constant	<0.01*	<0.01	-2.02	0.04
	n=135		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.86*	0.06	-2.03	0.04
White	0.59	0.55	-0.56	0.57
Male	4.41	5.01	1.30	0.19
Education	1.30	0.26	1.35	0.17
Constant	0.04	0.13	-1.10	0.27
	n=169		* = p<0.05	

In the Forgery group (Table 8), the statistically significant odds ratio for the White variable in the state sample is 2.64. This means that if a computer criminal in a state prison is white (non-Hispanic), they are roughly 164% more likely to have been convicted of computer assisted forgery. In the Federal sample of the Forgery group, the statistically significant odds ratio for Male is 0.31. This means that if a Federal prisoner convicted of cybercrime is a male, the odds of them being convicted for computer assisted forgery are decreased by roughly 69%.

Table 8. Forgery

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.98	0.01	-0.85	0.39
White	2.64*	0.99	2.57	0.01
Male	0.53	0.20	-1.66	0.09
Education	0.92	0.06	-1.07	0.28
Constant	5.03	5.45	1.49	0.13
	n=135		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.99	0.01	-0.09	0.92
White	0.89	0.30	-0.33	0.74
Male	0.31*	0.10	-3.43	<0.01
Education	0.91	0.06	-1.36	0.17
Constant	4.65	4.67	1.53	0.12
	n=169		* = p<0.05	

There were no statistically significant variables in Vandalism (Table 9) and the Intellectual Property Theft (Table 10) groups. The White variable was automatically omitted from the state sample in the Vandalism group by the statistical analysis program due to a collinearity issue. Once again, these analyses are based on very small sample sizes with very small variation. They are presented here in the hopes that future researchers will do a more in-depth investigation with a larger sample group or a different statistical method.

Table 9. Vandalism

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.87	0.09	-1.24	0.21
White	Omitted			
Male	1.73	2.20	0.43	0.66
Education	1.25	0.30	0.95	0.34
Constant	0.07	0.31	-0.63	0.52
	n=77		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.85	0.08	-1.58	0.11
White	1.74	2.36	0.41	0.68
Male	1.41	1.83	0.27	0.78
Education	1.14	0.31	0.48	0.62
Constant	0.36	1.39	-0.26	0.79
	n=169		* = p<0.05	

Table 10. Intellectual Property Theft

State Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.92	0.05	-1.51	0.13
White	2.05	1.82	0.81	0.41
Male	0.42	0.37	-0.96	0.33
Education	1.29	0.22	1.49	0.13
Constant	0.01	0.04	-1.53	0.12
	n=135		* = p<0.05	

Federal Sample	Odds ratio	Std. Error	Z	P>|Z|
Age	0.93	0.04	-1.57	0.11
White	1.37	1.07	0.41	0.68
Male	2.68	2.27	1.17	0.24
Education	1.13	0.17	0.79	0.43
Constant	0.04	0.10	-1.34	0.18
	n=169		* = p<0.05	

V. DISCUSSION

The main analysis for this study showed that all four independent variables were statistically significant in at least one of the two samples (Federal or state). The first variable, age, was hypothesized to have a negative relationship with computer crime, meaning that as people age, they are less likely to be computer criminals. This hypothesis was confirmed by the statistical analysis of both the Federal and state prison samples. In both cases, the computer criminals were significantly younger than their criminal counterparts in the sample, which coincides with the commonly held stereotype of hackers being young people. This stereotype stems from the early hacking community, which was mostly made up of young college students. After computers became more of a household item, it was the young people who had the time and inclination to learn about the new machines. This pattern of young people being more involved with computers throughout the evolution of computer technology seems to still be applicable today.

The race variable was greater than one in both the Federal and State samples, meaning that computer criminals were much more likely to be white (non-Hispanic) than other criminals. This variable was only statistically significant in the Federal sample, however. In the Federal sample, white (non-Hispanic) prisoners were 53% more likely to be computer criminals than other races. This also conforms to the commonly held beliefs about who hackers are. The early hackers and computer users in general were all Caucasians due to the fact that the first computers were found in places like major universities and large businesses that were overwhelmingly staffed by Caucasians at the time. This racial divide seems to have persisted into the modern age, with minority races

being much less likely to be convicted and imprisoned for computer crime than for other crimes.

The education variable showed evidence that the stereotype about computer criminals being more educated than other criminals may hold some truth. In both the Federal and state prison samples, the education variable was larger than 1 (1.35 and 1.51, respectively), meaning that every year of education increases the chances of being in prison for computer crime rather than non-computer crime. This variable was statistically significant in both the state and Federal samples, which means that for every year of education the prisoner has, their odds of being in prison for computer crime increase significantly. This stereotype began because early computer users were either attending universities or had white collar jobs that required higher levels of education. There may be an overlapping or interaction effect with social class and income, and further research into this area should attempt to find out how education, income, and computer crime actually interact.

The most surprising result of this analysis was the statistically significant effect of the gender variable, but in the opposite direction of that predicted in the hypothesis. The values for the gender variable were 0.29 and 0.44 in the state and Federal samples, respectively. This means that if the prisoner is male, their odds of being in prison for computer crime are very significantly reduced. The stereotype of computer criminals is that they are overwhelmingly male, but these datasets show that this stereotype may be inaccurate. Keep in mind that the data does not say that there are more female computer criminals than male computer criminals, merely that the percentage of computer

criminals that are female is significantly higher than the percentage of other criminals that are female.

The reasons for this are not immediately apparent, but the reason for the increased percentage of female computer criminals may be similar to the reason for the increased percentage of females in crimes like check fraud. Steffensmeier (1996) discusses many of the differences in female and male offending and offers some possible reasons for those differences. There is a large amount of research into the possible reasons for gender differences for crime in general and for specific crimes such as check fraud and shoplifting. Further research should be undertaken to attempt to link the gender imbalance of computer crime with the previously identified crimes in which females have higher than normal representation.

These comparisons of computer criminals and other criminals show that three of the four stereotypes being tested demonstrate some evidence of being based on reality, while the fourth stereotype seems to be completely contradicted. The subsequent analyses of variation within the computer criminal group also showed some very interesting results. People convicted for unauthorized access to financial information, identity theft, cyber trespassing, and copyright infringement were all significantly younger than their computer criminal peers in at least one of the two samples. This list of crimes represents a list of both easy to commit computer crimes and the more difficult to commit computer crimes, as discussed in Chapter 2. It would stand to reason that the more technically challenging crimes may be committed by slightly older computer criminals due to the increased time required to master those particular techniques, but this seems to not be the case.

The prisoners convicted of obscene communication were the only group to have significantly higher age, and this only applied in the state prison sample. They had an odds ratio of 1.09, which means that they every one year increase in age increases the odds of a state prisoner being convicted of obscene communication by 9%. The Federal prisoners convicted of obscene communication were the only group to be significantly more male. They had a statistically significant odds ratio of 4.24, which means that if the computer criminal is male, they have a 324% higher chance of being convicted of obscene communication rather than another computer crime. These two findings give some credence to the stereotype of the "dirty old man" sending sexually explicit messages to underage internet users.

The only group that was statistically different on the race variable was the state prisoners in the Forgery group. These prisoners had an odds ratio of 2.64, meaning that white, non-Hispanic computer criminals are 164% more likely to be in prison for computer assisted forgery than their non-white or Hispanic computer criminal counterparts. From the review of the literature on the subject, there is no stereotypical reason as to why those convicted of forgery should be more likely to be white (non-Hispanic) than their computer criminal counterparts, so more research will be needed to determine if there is an actual reason behind this racial difference or whether this is merely a statistical quirk that does not accurately reflect the population.

The only group to have a statistically significant lower chance of being male was the Forgery group in the Federal sample. This group had a 0.31 odds ratio, meaning that if the prisoner is male, they had a 69% lower chance of being in prison for forgery. As noted above, one of the reasons computer criminals may have a higher percentage of

females than other criminal groups is that computer crime may have similarities to check fraud or shoplifting, which also have a much higher percentage of female offenders (Steffensmeier, 1996). It would seem from this data that one of the major factors behind computer criminals having a higher percentage of female offenders is that computer-assisted forgers are much more likely to be female. Further research should attempt to determine just how much of the gender difference in computer crime is caused by the gender difference in specific computer crimes like forgery.

The only group to have a statistically significant difference in their education level was the prisoners convicted of copyright infringement, but only those in the state sample. The 1.68 odds ratio for this group means that for every one year increase in education, the odds of being a computer criminal in prison for copyright infringement increases by 68%. As with the forgery group being more likely to be white (non-Hispanic) there is no readily apparent theoretical basis for why those in prison for copyright infringement would be more educated than those in prison for other computer crimes. This result should be explored in further research to determine whether those in prison for copyright infringement are actually more educated than other computer criminals or if this result is merely a statistical quirk unique to this particular sample.

Overall, this research shows a lot of support for the stereotypes concerning computer criminals. The data about these prisoners seems to support the notion that computer criminals are younger, more educated, and less racially and ethnically diverse than their criminal counterparts. They also seem to be more female, which is the opposite of what stereotypes about hackers would have one believe. When comparing subsets of

computer criminals some interesting results are found, but it is difficult to make firm conclusions using such small sample sizes.

Limitations

There are many limitations to this research, as there are with all research. One aspect of this research that may influence the conclusions is that the data was gathered in 2004. The intervening ten years between when the data was gathered and this analysis may obscure any modern changes in the computer criminal subculture. One of the interesting pieces of information gathered from the literature review was that computer culture in general and hacker culture in particular are in constant flux. Even a small number of years could have changed computer culture in fairly significant ways. It is possible that more modern data could show that computer criminal culture has changed in meaningful ways in the intervening decade. From the literature review, it is clear that computer criminals are becoming older, more female, less white, and less educated over time. It is unclear how quickly this trend is affecting the computer user and computer criminal population, but a span of 10 years may well have caused significant change. The dataset for this analysis came from a survey that is performed every few years, and the 2004 version was the latest version at the time of this study. A new survey was conducted in 2012, but the results and data have not been published as of the time of this writing.

Another issue with the research is the wording of the question used as the dependant variable for the main analysis. The question asked "Did you use a computer to commit or help you commit the [CONTROLLING OFFENSE]?" The context of the question implies that the questions is attempting to measure cybercrime, but there may be individuals who did not understand what the survey makers were attempting to measure

with that question. Offenders who committed a crime with the assistance of a computer (selling drugs and keeping records of their sales online, getting online map directions to a store they robbed, using e-mails to set up a car theft, etc.) that would not be classified as cyber crimes may have answered "yes" to this question and been added to the "cybercriminal" group for purposes of the main analysis. Without an agreed upon definition of "cyber crime" (as discussed in Chapter 1) the issue of accurately measuring computer criminal activity will affect all studies that attempt to quantify it.

A third issue is a problem of selection. The only criminals used in this analysis were criminals that have been caught, prosecuted, and imprisoned for that crime. Because of this selection issue, conclusions may not be accurate for offenders in general. If the subset of criminals who are arrested, tried, convicted, and imprisoned for computer crimes are different from computer criminals in age, gender, race, or education, this will bias the dataset and result in biased statistical conclusions. Unfortunately, there is no way to assess a representative and random sample of computer criminals that have not been caught, because by definition anti-government criminal subcultures do not have openly available membership lists.

VI. CONCLUSION

This research set out to investigate commonly held beliefs about who computer criminals are. There are numerous stereotypes about computer criminals that are found in numerous forms of media and even peer reviewed academic journals and scholarly works. The authors of these works seem to assume that the stereotypes are true or cite statistics from decades previous, assuming that those same trends still hold true today. This research quantitatively examined these stereotypes using a modern dataset from a large prison survey.

The results showed that three of the four stereotypes tested may have some basis in reality. Computer criminals in the sample were more educated, younger, and less racially and ethnically diverse than their criminal counterparts. The results also showed that computer criminals were much more likely to be female than their counterparts, which goes against the mainstream view that computer criminals are overwhelmingly male. Some further analysis comparing subsets of computer criminals found that there are certain distinct differences in different types of computer criminal groups, but these results will need to be investigated further and verified using larger sample sizes. Computer crime is a problem that will grow along with the growth in computer ownership and use around the world. As computers become more and more popular and are put into more devices every year, computer crime will start affecting more people and it will affect those people not just through a traditional desktop computer, but through their cars, their phones, their televisions, and even their books. Finding out who computer

criminals are is an important step in catching them, rehabilitating them, or even preventing their becoming a computer criminal in the first place.

REFERENCES

Arnell, P. & Reid, A. (2009). Hackers Beware: The Cautionary Story of Gary McKinnon. *Information & Communications Technology Law*, 18(1), 1-12.

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (2007). *Cybercrime: Digital Cops in a Networked Environment.* New York: New York University Press.

Blankenship, Lloyd. (1986). The Hacker Manifesto. *Phrack,* 1(7).

Coleman, G. (2011). Hacker Politics and Publics. *Public Culture*, 23(3), 511-516.

Denny, R. T. (2010). Beyond Mere Theft: Why Computer Hackers Trading on Wrongfully Acquired Information Should be Held Accountable Under the Securities Exchange Act. *Utah Law Review, 2010*(3), 963-982.

Dudek, D., & Johnson, N. (2011). Return of the Hacker as Hero: Fictions and Realities of Teenage Technological Experts. *Children's Literature in Education*, 42, 184-195.

Gutmann, E. (2010). Hacker Nation. *World Affairs*, *173*(1), 70-80.

Halbert, D. (1997). Discourses of Danger and the Computer Hacker. *The Information Society*, 13, 361-374.

Hoar, S. (2005). Trends in Cybercrime: The Dark Side of the Internet. *Westlaw*, 20(4), 1-13.

Jacobellis v. Ohio, 378 U.S. 184 (1964)

Jaishankar, K. (Ed.) (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Florida: CRC Press.

Jamil, D., & Khan, M. (2011). Is Ethical Hacking Ethical?. *International Journal Of Engineering Science & Technology*, *3*(5), 3758-3763.

Levy, S. (2010). *Hackers*. California: O'Reilly Media, Inc.

Mitnick, K., & Simon, W. (2002). *The Art of Deception*. Indianapolis: Wiley Publishing.

Mitnick, K., & Simon, W. (2006). *The Art of Intrusion*. Indianapolis: Wiley Publishing.

Mitnick, K., & Simon, W. (2011). *Ghost in the Wires*. New York: Little, Brown and Company.

Moon, B., McClusky, J., McCluskey, C., & Lee, S. (2012). Gender, General Theory of Crime and Computer Crime: An Empirical Test. *International Journal of Offender Therapy and Comparative Criminology*, 57(4), 460-478.

Nikitina, S. (2012). Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture. *The Journal of Popular Culture*, 45(1), 133-152.

Nissenbaum, H. (2002). Hackers and the Battle for Cyberspace. *Dissent, 49*(4), 50.

Nykodym, N., Kahle-Piasecki, L., Ariss, S., & Toussaint, T. (2010). Cybercrime and Business: How to Not Get Caught by the Online Phisherman. *Journal of International Commercial Law and Technology*, 5(4), 252-259.

Olson, P. (2012). *We Are Anonymous*. New York: Little, Brown and Company.

O'Neil, M. (2006). Rebels for the System? Virus Writers, General Intellect, Cyberpunk and Criminal Capitalism. *Continuum: Journal Of Media & Cultural Studies*, *20*(2), 225-241.

Steffensmeier, D. & Allan, E. Gender and Crime: Toward a Gendered Theory of Female Offending. *Annual Review of Sociology, 1996.* 22:459–87.

Thomas, D. (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.

Verton, D. (2002). *Confessions of Teenage Hackers*. Berkeley: McGraw-Hill.

Victaulic Co. v. Tiemann, 499 F.3d 227 (2007)

Wark, M. (2004). *A Hacker Manifesto.* Cambridge: Harvard University Press.

Warnick, B. R. (2004). Technological Metaphors and Moral Education: The Hacker Ethic and the Computational Experience. *Studies In Philosophy & Education, 23*(4), 265-281.

Winmill, B., Metcalf, D., & Band, M. (2010). Cybercrime: Issues and Challenges in the United States. *Digital Evidence and Electronic Signature Law Review*,7, 19-34.

Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet Initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings from a National Study. *Journal of Adolescent Health*, 35, 424e11-424e20.