OVERVIEW AND THEORIES OF CYBER CRIME

By

Caden Charles Johnson

A Research Paper

Submitted to the Faculty

Of

St. Cloud State University

In Partial Fulfillment of the Requirements

For CJS-486/ Theories of Crime and Justice

St. Cloud, Minnesota

December, 2019

INTRODUCTION

This research paper examines the overview and theories of cyber crime. Theoretical explanations and the research literature are used to answer four principle research questions. Those queries were further refined by supporting questions as follows.

(1) What is the historical background of cyber crime?

1a. When did it begin or when was it first noted?

1b. Who were the key players?

1c. What was the etiology (i.e., cause and distribution)?

(2) What is the nature and extent of cyber crime?

2a. What are they doing and who is involved?

2b. When and where are they doing it?

2c. How are they doing it and why?

2d. How often and how much of it are they doing?

(3) What has been the response to cyber crime?

3a. What has been society’s response?

3b. What has been the criminal justice system’s response?

(4) What recommendations can be made regarding cyber crime?

4a. What more can or should be done?

4b. What is the future going to look like, how will it change?

HISTORICAL BACKGROUND

The idea of hacking first originated from MIT when a couple of their students modified model trains. They tried to change their functions and how they worked without actually physically changing anything on them. From there, things have definitely come a long way. With the rise of technology, people began changing computer codes to fit their desired purpose. As Florida Tech states, “The malicious association with hacking became evident in the 1970s when early computerized phone systems became a target. Technologically savvy individuals, called “phreakers,” discovered the correct codes and tones that would result in free long-distance service. They impersonated operators, dug through Bell Telephone company garbage to find secret information, and performed countless experiments on early telephone hardware to learn how to exploit the system and steal long-distance telephone time.” (floridatechonline.com, 2019).

From there the name hacker moved to anyone who could or would manipulate electrical signals, computer programs, or other aspects of technology most often out of malicious intentions. In today’s society, cyber crime acted out by hackers is often seen behind the screen of a computer creating programs or scripts and trying to find loopholes in systems, tricking people into giving something up, or gaining access to things they shouldn’t have access to. As you can see, cyber crime quickly emerged from the innocence of model trains, and since then has become a way to steal, lie, and manipulate the outside world from a computing device.

Key players in these crimes are known as “hackers” or malicious actors. They gain access, alter code, or act sneakily on the web in order to steal, manipulate, or destroy. These people in today’s society can range from someone who is living in their parent’s basement, all the way to government employed hackers trying to gain access to classified documents through devious means. In the sense of actual crimes being committed by regular citizens or criminals, cyber crime has been committed by a vast amount of people and often can not be traced back to who committed it in the first place. One of the first Offences ever seen for cyber related crime was in 1983 by six teenagers in Milwaukee that hacked the computers belonging to Alamos National Laboratory, Security Pacific Bank, and Sloan-Kettering Cancer Center. One of those teenagers was eventually given 2 years of probation (nytimes, 1984). Another one of the first documented criminalization of these offenses was in 1986 by Robert Morris, who was a student at Cornell University and created the “Morris Worm”. This worm damaged thousands of computers and cost around $98 million dollars in damage. Congress passed the Federal Computer Fraud and Abuse Act that “made computer tampering a felony crime punishable by significant jail time and monetary fines” (floridatechonline.com, 2019). The other key players in these crimes are also obviously the victims. Whether it be an innocent person, a corporation, or a government, the results can be devastating and cost not only a huge loss of money but also of data, and ultimately trust in technology.

Another example of a well-known hacker and key player is Kevin Mitnick. “Using the alias "Condor," Kevin Mitnick's first big hack was a Department of Defense computer, which he gained access to when he was only 16 years old. His most famous crime in his younger days was stealing $1 million worth of software from computer company Digital Equipment Corporation (DEC). So when the FBI began investigating him in connection with a hack of the California Department of Motor Vehicles in 1992, he was determined not to get caught again and made a run for it. While a fugitive from the law, Mitnick continued to use a laptop and cell phone to break into computer networks and telephone systems across the country, stealing software, files, access codes, and anything else he could get his hands on, including some 20,000 credit card numbers.” (Lammle, 2011). He ended up spending over 5 years in prison but ended up spending 8 months in solitary confinement.

The cause of the very first initial crime, and a vast majority of other cyber related crimes thereafter can be affiliated with the curiosity attached to the endless possibility that technology provides. I will later (in section 2-Nature and Extent) go over the theories of why people choose to commit these crimes, but for now, the cause and distribution of cyber crime from the beginning has been due to the access to technology and the education or knowledge of how to manipulate it. The first examples of these crimes often stemmed from universities due to the abundance of technology and the curiosity of students who did not understand the implications and consequences of these dangerous actions.

The introduction of such powerful and intriguing technology and the connections that linked them contained many avenues of exploration, and once discovered, led to even further discoveries of exploits and vulnerabilities to manipulate it. This process of exploration served two purposes though. The crimes themselves were wrong and punishable, but in the end led to solutions in how to prevent against such attacks and possibly further ones. Even today, a valuable career field is Penetration Testing, in which you legally hack the devices or networks belonging to your company or agency in order to find the vulnerabilities and solve them before they are found by someone else. It leads to a constant cycle of “cat and mouse” but in the end makes everything more secure by trial and error. The problem began when people started hacking for themselves and not for the benefit of security.

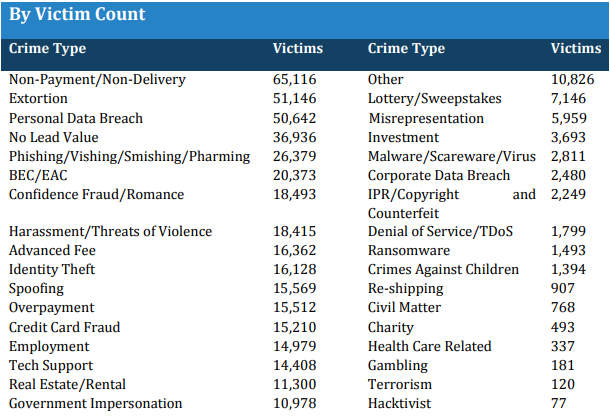
All of these crimes took place behind a screen, acted out by the computer, and sent over connecting media via electrical signals. This fairly new category of crime is like no other earlier crimes. It doesn’t include a weapon, very rarely is anyone actually physically hurt, and you don’t have to do very much physically to commit a criminal act. It can be completely untraceable and requires education or thorough knowledge on how the fundamentals of computing systems work. Cyber crime is not a crime that can be commit on accident such as trespassing or hitting someone with your car. It takes practice, planning, and dedication; if someone commits a cyber related crime, it is not a spur of the moment event.

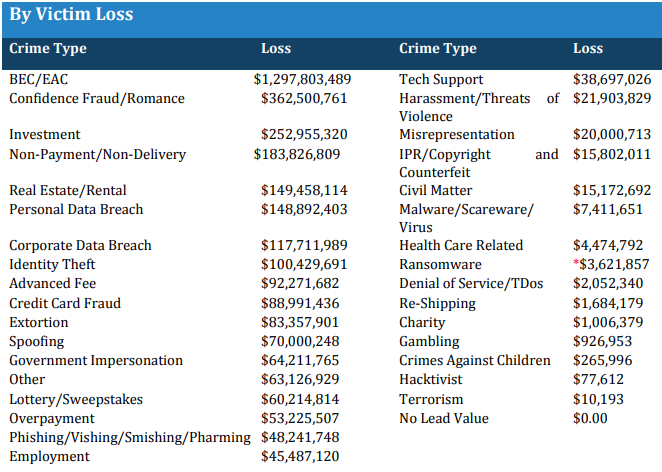
NATURE AND EXTENT

Types of cyber crime, like any other crime, differ depending on the motive and what access the malicious actor has. Motives can include, but are not limited to: money, revenge, information (such as documents), a sense of purpose, practice, and even just pure boredom. Most cyber related crime can be committed from a remote device anywhere in the world, but more direct attacks may also include gaining restricted access to either physical hardware or other people’s devices. Attacks including botnets can be acted out by gaining control of hundreds, thousands, or even hundreds of thousands of other unaware people’s devices and using them all to carry out a goal as shutting down servers by flooding them with data and requests over a network. This demonstrates how a criminal’s reach is much more expanded by the technology available. Cooperating with other hackers or even forming a hacking group would expand your reach even further but would also expand your skillsets which would come in handy if you were working on a large hack with many parts and over a long period of time. It really depends on the person committing the crime and what their motives are for carrying out the hack that determines who is involved and how long the preparation takes.

If a hacker’s motive is money, they may attempt to disguise themselves as another entity to get banking information, restrict access to your own system and files for ransom, and even trick you into buying things without ever intending to follow through with a sale. If the hacker’s motivation is instead information or data, they will use a technique called sniffing to intercept traffic and obtain things that you send or receive. There are too many motives out there to count, and with each one is a different attack or technique used to satisfy that motive. Additionally, these different attacks or techniques may have different sentences or crimes associated with them. For example, sniffing someone’s traffic will have a lot less jail time (if any) than hacking the actual device and obtain total control of it to steal files.

Also, depending on what the target is, the crime may be considered more severe or less severe. If you were to hack a wireless-accessible camera for a small business just for practice or for fun, the punishment if caught wouldn’t be very sever. But on the other hand, if you were to hack a wireless-accessible camera in a government building such as the pentagon or any other government building, it would be considered a lot more severe and would have much worse consequences attached to that crime. As you will see, there are a variety of crimes that can be committed via technology, and specifically the internet. Shown below is an image published by the Federal Bureau of Investigation for the number of victims of cyber crimes in 2018 and immediately following is an image from the same source for the monetary loss from those crimes in 2018:





(FBI, 2018)

Hackers are often alone in their attempts, and this is partly due to the very common stereotype of their personalities. Hackers have often been known to be introverted, and rarely work in groups, especially in criminally related attempts, except in some occasions. In the occasion of massive hacks, they can take years to complete and often are linked to hacker groups. These groups can either be regular criminal individuals, or they have been known to be government affiliated. Like I stated before, even without help, a hacker or malicious actor can gain help from other devices that they infect and arrange in a botnet to strengthen an attack. In the higher levels of attacks and deep into criminal culture, hacker groups in the 21st century can meet, communicate, and organize attacks on what is known as the “dark web”. The most popular and widely known group in the world is known as “Anonymous” which has not only carried out cyber elated crimes but has also carried out attacks in the pursuit of justice in a sort of “Robin Hood chivalry”. In the most notable hack carried out by the group in 2017, Anonymous took down over 10,000 child pornography sites and in the process affected around 20% of the dark web (Papenfuss, 2017). They had done similar attacks to this previously, but never that big. However, they also have demanded money before, stolen data, and even threatened a sitting US president (Donald Trump). This is just one example of a hacker group, but there are many more that are even more malicious. However, there is also a huge majority of hackers that work alone and do a lot of damage too.

Cyber crimes are being committed constantly, and all across the globe; malicious code is being sent and received even as I write this. All of these crimes, however, contain one thing in common; The access to technology and the knowledge of how to manipulate it is the key factor to commit these types of crimes. Not any criminal with a gun can hop on a computer and return with money, data, or restricted access. If mastered though, these crimes can be carried out from a different state, country, or even continent. On another note, the statistics at least show where the victims of these attacks are. Excluding the United States\*, India had the highest number of victims at 4,556 and Japan had the lowest amount of victims at 311 for 2018. These victims were the statistics taken from 2018, and only from the top twenty countries\* excluding the United States (FBI, 2018). Out of the top 10 states for victims of cyber crime, California was the only one over 30,000. However, California, Texas, Florida, North Carolina, and New York all lost over $100 million each just in 2018 (FBI, 2018).

From here, I’d like to go into the theories of why criminals may be carrying out these crimes. Theories of crime are various ideas/theories as to why people do what they do. These theories not only help find out why someone committed a crime but can also help us determine why someone may commit a future crime and how to prevent it. According to the Classical school of thought, there are many factors to take into consideration. Due to free will, these people are free to make their own choices, and since they are presented with the opportunity, are taking it. Since people are rational beings and weigh the costs and benefits of their decisions, cyber crime offers a lot of benefits and very few costs other than the necessary education and devices. In the sense of deterrence, there is close to none. Law enforcement agencies have made huge efforts to crack down on these crimes, but most often, the smarter a hacker is, the harder it is to trace who did it if even possible. I won’t get into extreme detail, but with the use of proxies and the dark web, it can be ensured that your activities are untraceable and unpunishable.

A huge theory that may coincide with cyber crimes is the Social Learning theory. Under the umbrella of this theory are the premises of imitation, differential association, differential reinforcement, and definitions. The general idea comes from this theory that if a hacker were to be working with a group, have contact with another group, or even learn from another hacker, the ideas about the crime and the skills from the others would influence this person to commit cyber crimes as well. The approving attitude towards the crime, the motivation, the realization of rewards, and even the skills could come from that outside source and further influence criminal activities. In accordance with Positivist theories, criminals are born criminals and are different from regular people. If this is the case, this may have an influence on why they take the opportunity to act out these crimes. Another theory that stood out to me was the Strain theory, which in essence, states that criminals may act out crimes due to lack of education or poverty. Obviously, lack of education wouldn’t be the answer here, but Poverty and a lower income may influence people to turn to technology to attempt an attack with the motive of money. These attacks may involve ransomware or sniffing/spoofing in order to gain access to bank accounts or credit card information.

In response to the quantity and frequency of cyber crimes, it is a bit staggering. According to the Center For Strategic and International Studies, there have been 16 major attacks alone in the month of October, 2019 (csis.org, 2019). These attacks are only the biggest and the ones worth mentioning. Following is an example of a hack that took place only two months ago: “Iranian hackers conducted a series of attacks against the Trump campaign, as well as current and former U.S. government officials, journalists, and Iranians living abroad.” (csis.org, 2019). Although they only posted these hacks on their site in 2019, some of these hacks have had campaigns that go all the way back to 2013. Also, a lot of cyber conduct, whether illegal or otherwise, is often conducted by government related groups or persons, so it can get quite messy. Another example of how cyber crime influences today’s society is displayed by Cybersecurity Ventures’ 2019 Official Annual Cybercrime Report. It states, “In August of 2016, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.” (Morgan, 2019).

To sum up the question of how often it is happening and how much of it, It is going on constantly, and it is a staggering amount. Some cyber criminals even set up programs or bots to continuously run code in attempts to infect hosts (people’s devices). This can be seen in examples such as worms and viruses. A worm built by a hacker will infect computer after computer and install viruses. It will then use that computer’s connections, contacts etc. to connect and infect other hosts and then repeat. The virus, once installed and activated can do a variety of things, all of which are illegal. This ability to cause widespread chaos and sometimes without even being noticed is why cyber crime is so difficult to track down, determine a sentence for, and charge someone with a specific crime.

A very interesting aspect is the statistics of different victims per age group. In the FBI annual crime report from 2018, there were only 9,129 victims under the age of 20, and they lost a total of $12,553,082. On the other hand, there were 62,085 victims over the age of 60 and they had a total loss of $649,227,724 (FBI, 2018). This might have to do with the younger generations being more “tech savvy” and more careful on the web compared to older generations. Also, a lot more attacks have been targeted towards older generations, and the scams/spam can be directed to people of certain ages due to certain saved data, cookies, or saved preferences.

THE RESPONSE

With the rise of technology including handheld devices, social media and IOT (Internet of Things) devices, society has become extremely vulnerable to malicious actors, and a huge amount of people have become victims to fraud, identity theft, etc. With these growing concerns, companies have emerged with security solutions such as encryption, password protection, and secure connections. Operating systems such as Windows, Apple, and Linux have come out with virus detection software and many other third party sources offer different virus scans and such for a price. Additionally, VPN’s (Virtual Private Network) can be purchased through a large variety of companies, and these help to provide encrypted and safe connections to the internet.

Society has become accustomed to the dangers of technology and it has become common knowledge to anyone on the web to never click on random ads or messages from unknown sources. People have spoken out and victims have been able to contact law enforcement such as the FBI or NSA for large threats that may impact the rest of the population. Private companies specializing in cyber security have become a necessity and are employed by large corporations and government agencies in order to help prevent against attacks. Slowly people have adapted to the threats, but as long as there are computing devices and networks connecting them, it will only get worse.

In respect to the criminal justice system, higher levels of law enforcement and intelligence agencies such as the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Central Intelligence Agency (CIA) have become the main combatants against cyber crime. However, some smaller law enforcement agencies who can afford it have become employing cyber security teams. From my personal experience, this is not enough. A lot of cyber crimes go unnoticed and the criminals are never caught in smaller attacks and especially when the only criminal justice system available is a small-town police force. Attacks such as these are not physical and cannot be caught using witnesses and normal investigation. An experienced cyber security professional is the only person that can find out what really happened and can have a chance to find out who committed the crime.

Due to the vast and immense size and structure of the dark web, traffic and attacks can become untraceable and it has become a hub for criminal activity with cyber crime as only a small part, but the founding principle. This amazing technology has sadly allowed a place for drugs, guns, and even people to be purchased and sold. The criminal justice system has only put a dent in the danger that is present. Another major problem is the lack of statistics when it comes to cyber crime. All of the estimations published by the FBI, NSA, etc. are simply just that: estimations. Without actual arrest numbers and numbers of total attacks, it is very difficult to determine how well the criminal justice system is doing in handling the problem. After thorough searching for statistics related to annual arrests, I was only able to find the victim statistics shown previously in section 2 (Nature and Extent).

RECOMMENDATIONS

In regards to what further steps can be taken to protect and prevent against cyber crimes, education is key. The main difference between the statistics shown earlier between the age groups of victims is the fact that the younger generation has been made aware that the internet is not a completely safe place. Growing up with the technology and with the knowledge of the risks has decreased their chances of being victims due to safer practices. Education of older generations and even the entire public about the risks of technology vulnerabilities and the preventions you can take would make a huge impact in the number of victims to cyber crime each year. This will inevitably decrease dollars lost to these crimes as well. Another improvement would be to standardize the sentences for the various types of cyber crimes. After lots of research and reading into the state of Minnesota’s view on computer related internet crimes, I was not able to find any distinguished sentences or consequences for any of the crimes. The courts often have jurisdiction over what the offender will receive as a sentence, but a semi-standard set of consequences or sentences may help serve as a deterrence to make criminals rethink whether they want to commit the crime.

Additionally necessary, cyber security should become even more of a requirement, and more law enforcement agencies (especially small towns and cities cyber support) should employ or contract out cyber security specialists to helps prevent against attacks and to help crack down on attacks that do occur. Furthermore, offensive cybersecurity specialists would be very resourceful if used to find the hackers breaking the law and helping arrest them before the commit worse crimes. This will not only help with general deterrence to prevent other crimes but will save possible future victims and their money. Cyber crime is a generally new class of crime since it’s only been around for less than a century. Inevitably in the future, it will need to be classified and standardize throughout the country along with distinguished restrictions and consequences. Along with this, there will need to be a widespread education on how to not only be safe with technology and protect yourself, but also how to be responsible with the technology given to us and how to not cross the line into crime.

The world is growing every day, and with growth comes change. Technology will advance, more vulnerabilities will unravel, and more attacks will be made. With this new world of possibilities, I can see technology becoming more and more integrated into everyday life. With that, cyber crimes will strike closer and closer to home and will become even more dangerous. Following this, the monitoring and cracking down on cyber crime will inevitably become more important and more common in everyday life. For example, self-driving cars, smart homes, and other powerful IOT devices, although seemingly safe, are all vulnerable and have plenty of exploits that can turn them into harmful devices and even possibly dangerous to the extent of fatal. Imagine if your self-driving car was hacked by a malicious actor through the car’s wireless internet, and your brakes lock up in the middle of a highway or the steering wheel is ripped to the side. These things, if the software isn’t up to date and connections aren’t managed wisely, can become a huge step for cyber crime toward more serious effects and danger for the rest of the population. The further technology is integrated into daily life and the more we rely on it for important things, the more dangerous it can become if we don’t control cyber crime.

Crime has been a problem since the dawn of time and will not end anytime soon. There is a possibility that cyber crime may decrease if steps are followed and policies are put into place. However, things may go the other way. For all we know the future may hold something similar to George Orwell’s idea of a future society ruled by technology in his novel “1984”. Either way, we have the responsibility to do our best to prevent crime and protect law abiding citizens, and with the adaptation of the criminal justice system to the ever growing world of technology it will be able to do what it has always done.

CONCLUSION

In a world of continuous technological growth, the opportunities for crime have increased and the effects of these crimes have become more devastating. Cyber crime is defined as any crime that occurs online or through the use of a computing device. Due to the vast networks connecting today’s devices and people, these crimes can violate people’s privacy, threaten government security, and take down businesses. It has become a huge problem and will only get worse. However, although we know what these crimes are and how they are committed, we need to thoroughly understand why the cyber criminals do what they do. Not only do we need to understand that, but we also need to be vigilant and safe in all technology related practices. Cyber security has become a necessity and as more vulnerabilities become available, it is the responsibility of those working in this field to protect and prevent against attacks from cyber criminals.

BIBLIOGRAPHY / WORKS CITED

(csis.org, 2019), Significant Cyber Incidents. (2019). Retrieved 2019, from https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

(Papenfuss, 2017) Papenfuss, M. (2017, February 7). Anonymous Hackers Take Down 10,000 Dark Web Sites. Retrieved from https://www.huffpost.com/entry/anonymous-hacker-takes-down-10000-dark-web-sites\_n\_5899785ae4b0c1284f27ebb3.

(floridatechonline.com, 2019), A Brief History of Cyber Crime. (2019, December 11). Retrieved from https://www.floridatechonline.com/blog/information-technology/a-brief-history-of-cyber-crime/.

(Morgan, 2019), Morgan, S. , “2019 Official Annual Cyber Crime Report”, Retrieved from <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>

(FBI, 2019) Federal Bureau of Investigation. “2018 Internet Crime Report.” 22 June 2018,  <https://pdf.ic3.gov/2018_IC3Report.pdf>. Accessed 12/12. 2019.

(nytimes, 1984), The New York Times Archives, Ap. (1984, May 1). Computer User Sentenced. Retrieved from https://www.nytimes.com/1984/05/01/us/computer-user-sentenced.html.

(Lammle, 2011), Rob Lammle, January 3 2011, “4 Famous Hackers Who Got Caught”, <https://www.mentalfloss.com/article/26767/4-famous-hackers-who-got-caught>