Themis: Research Journal of Justice Studies and Forensic Science

Volume 6 Article 10

5-21-2018

An In-Depth Look into Cybercrime

Brandon McDaniel
San Jose State University

An In-Depth Look into Cybercrime

Abstract
Cybercrime is an increasing area of study in the field of criminology. With the advancement of technology and the growing use of social media, people are connected all over the world more than they have ever been before. It is not the invention of new crimes but technology has allowed old crimes to be committed through a new medium. This paper explores the realm of cyberspace and how old crimes are being committed in new ways by different countries and people.

Keywords
cyber crime, internet, social media, technology

An In-Depth Look into Cybercrime

Brandon McDaniel

Abstract

Cybercrime is an increasing area of study in the field of criminology. With the advancement of technology and the growing use of social media, people are connected all over the world more than they have ever been before. It is not the invention of new crimes but technology has allowed old crimes to be committed through a new medium. This paper explores the realm of cyberspace and how old crimes are being committed in new ways by different countries and people.

Introduction

Cybercrime is a growing and increasingly important subcategory in criminology. The objective of this paper is to explore the different aspects of cybercrime, and how it relates to criminality. Cybercrime is a marginalized component of criminology because it does not take place in the physical space, but in the cyberspace (Ngo & Jaishankar, 2017). Researchers are having difficulties getting their research published because academics in the American Society for Criminology have not agreed upon the methodologies developed for studying cybercrime (Diamond & Bachmann, 2015).

Cybercrime generally involves employment of deception using a computer for the prospect of financial gain such as, identity theft, engaging in the distribution of child pornography, selling and buying drugs, or any other illicit and illegal activity (Ophardt, 2010). Cybercrime can be sorted into two types of methods; the first being that the computer is used as a tool to commit a crime, and the second is when the computer is the target of the crime (Diamond & Bachmann, 2015). What is left out is the "user", or the criminal who is committing the act.

Statistically speaking, men and women commit cybercrime equally (Donner, 2016). That being said, cybercrime is not gender specific. Cybercrime is costing the world economy up to one trillion dollars a year, which affects consumers, businesses, and financial institutions. To prevent a victim's funds from being stolen there are costs to protecting themselves from attacks, purchasing antivirus software and keeping hardware up to date is expensive (Ngo & Jaishankar, 2017). Fraud is the leading cause of cybercrime in Canada. It makes sense why many people in the world are losing money since fraud is a simple way to get money from an unsuspecting victim

(Mazowita, 2014). According to Ngo and Jaishankar (2017) since 2013, 40% of the world has had access to the internet, and they estimate that about 100 people have gained access to the internet every day since then. The more people online, the more opportunities are created for criminals to access people's information and use that information for their personal gain at the expense of their victims.

According to Conteh and Royer (2016), cybercrime is a low-risk crime compared to physically going into a business or someone's house. Using a computer as their vehicle, the criminal can attack their target from a location they feel safe in. When committing a crime in person, there are many traces of physical evidence that can be left behind, but for hackers covering up their tracks it is relatively easy¬—even for inexperienced hackers (Conteh & Royer, 2016). They do not have to worry about leaving DNA or hair behind at the scene of a crime, and they can hit multiple targets in seconds (Conteh & Royer, 2016). These are some of the many ways hackers commit cybercrime and why it is such a difficult problem for law enforcement to combat.

Literature Review

State Sponsored Cybercrime

State sponsored cybercrime is a new means for countries to undermine and disrupt each other. Tactics utilized are like those used during the Cold War era with goals of causing their enemies confusion, and disorientation. State sponsored cybercrime is not always considered a crime in the state that is doing the attacking, but it is often considered a crime in the country that is receiving the attacks (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014). Crime is a social

construction, therefore open to interpretation by different cultures.

The first time a state sponsored cyber-attack occurred simultaneously with an armed conflict was in 2008, when Georgian and Russian soldiers clashed in the South Ossetia region (Ophardt, 2010). Cyber warfare was used as a weapon and tactic in this conflict. Cyber Warfare is the use of computer systems to disrupt an intended target's computer system infrastructure. Denial of Service is a type of attack that a user can utilize to attack an intended single target to flood their computer with fraudulent requests, overwhelming the computer and network (Ophardt, 2010). Distributed Denial of Service attacks are even more severe because it is the use of multiple computers to attack many targeted computers. This form of attack is challenging to defend against because of the use of malware, a computer virus that affects the software of a computer without the user or the computer knowing the computer is infected (Ophardt, 2010).

Most recently, actors from the Russian government have been implicated in hacking into the Democratic National Convention and stealing emails related to the 2016 presidential election (Kerr & Murphy, 2017). Kerr and Murphy (2017) have also given examples of North Korean hackers breaking into the files of Sony because they produced a movie that ridiculed North Korea's supreme leader; they also posited that the United States and Israel were behind a cyberattack that shut down an Iranian power plant's centrifuges.

The United Nations has not recognized the actions of state sponsored cybercrime as being an issue they need to address, because they believe conflict can ensue if a country's population or an individual citizen of a country is labeled a

criminal (Broadhurst et al., 2014). The United Nations' reluctance to address the problem of state sponsored cybercrime is disconcerting. If nation states are not held accountable for their actions, then how can we expect to deter individuals from committing cybercrime? The United Nations is hesitant to take action against individuals or nation states because nations have different laws about cybercrime; what is legal in one country is illegal in another (Broadhurst et al., 2014).

Organized Crime and Online Organized Crime

Organized crime groups are increasingly prevalent in the growing age of information technology (Broadhurst et al., 2014). Cybercrime can be committed by individuals who wish to disrupt and cause mayhem, but an organized group of individuals seeking to cause disruption is more effective. Calling these online groups organized crime has confused many into thinking they are the traditional organized crime syndicate like the mafia (McCusker, 2006). McCusker (2006) argues that it would seem logical and pragmatic that such a group would evolve into using cyberspace to earn their money. According to the Council of Europe, data of organized crime groups committing online crimes do not show that they have made a transition into cybercrime. They cannot tell if they were criminals who got together online or if they happened to be criminals working online separately (McCusker, 2006).

It is logical that an organized crime group would want to expand their operations to make as big of a profit as possible, but McCusker (2006) is saying that it is not practical for a criminal organization with a top down hierarchy system of management to change the way they operate and take on a new form of criminality. What confuses people about organized cybercrime is the multiple attacks that a group of hackers make while working

together to attack their targets (McCusker, 2006). It is not necessarily a single uniformed group like the Italian mafia making an attack (McCusker, 2006). It is a web of individuals that do not belong to a certain group, but instead are working together to achieve a common objective.

The Dark Web

The dark web is a separate entity than your average search engine such as Google or Yahoo because it is not accessible through these systems (Martin, 2014). Originally, the internet was designed for the transfer of data information (McCusker, 2006). Its limitations were boundless as the ability to send and receive more information grew as technology advanced. The internet was not designed to be secure, and its ability to rapidly exchange information has been a hurdle for law enforcement to keep secure (McCusker, 2006).

Encrypted websites such as The Silk Road allow people to trade in illegal commodities like drugs, and other illegal paraphernalia (Martin, 2014). Martin (2014) explains that users log into the site like how someone would log into Facebook. The site is encrypted, so no one knows who or where the other person is because there is no face-to-face meeting. People can shop the site for merchandise like any other online store. A third-party administrator receives a percentage for handling the transaction. Encrypted currency like Bitcoin is used to exchange goods to further secure the transaction. Customers can even give a zero to five-star rating of how satisfied they are with their purchase, and they can leave feedback for other customers using this specific vendor (Martin, 2014).

The government has ways of finding these users on encrypted sites; they can hack into an administrator's computer by tricking them into downloading a code that will give away the

suspect's location and, hopefully, their identity (Kerr & Murphy, 2017). According to a research project by Barratt, Ferris, and Winstock (2014), drug users were less likely to use The Silk Road for fear of getting caught, which made the price of drugs cheaper in that market. Kerr and Murphy (2017) state that a drawback to law enforcement pursuing these offenders are the international relations that can be strained because of law enforcement prosecuting foreign nationals. It could lead to the prosecution of United States officials in other countries (Kerr & Murphy, 2017). Encrypted and hidden realms of the internet are where crimes are being committed and hidden from the general public.

Cyberbullying

Cyberbullying is a new form of bullying—although not physical, it can be used psychologically to intimidate and cause emotional distress. Men and women tend to bully in different ways because men generally use physical types of bullying (Marcum, Higgins, Freiburger & Ricketts, 2014). On the other hand, women use emotional and psychological forms of bullying, and are generally less confrontational in person. In the cyber world, physical violence cannot take place; therefore, it has been hypothesized that women are as prone, if not more, prone than men to commit cyberbullying. The ability of not having to be face-to-face with the person they are attacking, by using the computer screen as a barrier, makes the actions easier. Cyberbullying can have long lasting effects on a person such as suicidal thoughts, anxiety, and emotional stress (Marcum et al., 2014).

Marcum and colleagues (2014) conducted a survey at a college campus to better understand what factors influenced men and women to commit cyberbullying or be a victim of it. They

found that people with less self-control were more likely to engage in cyberbullying. Men who spent more time on social media built up a persona and were more likely to engage in cyberbullying. Moreover, they found that the more friends women had on social media, the more likely they were to gossip and be more prone to cyberbullying, especially if their friends were also cyberbullying. Being part of a large group that is involved in sending hurtful messages to people can give an individual confidence by being backed by their peers. They consider the most important finding to be that if people feel supported by their peers, they are more likely to interact in online bullying (Marcum et al., 2014).

Law enforcement has been slow to react to cyberbullying. Police do not respond until there has been a physical crime committed in the real world, not in the cybersphere (Broll & Huey, 2015). In a few cases, there have been events that were exploited on social media that have led to young people killing themselves due to cyberbullying (Broll & Huey, 2015). Criminal charges are brought against some of the people involved in cyberbullying that lead to someone taking their own life, but often the charges are withdrawn, and convictions are overturned on appeal (Broll & Huey, 2015). Bullying has been a rite of passage from youth to adulthood. Bullying had the potential to become criminal, but for the most part ends up being handled by the school. Cyberbullying generally takes place off campus, but some schools have overstepped their bounds by disciplining students for acts that did not occur on campus. These schools were reprimanded by courts because the courts believe they were infringing on students' rights. This made school administrators reluctant to get

involved in cyberbullying that was happening in their school (Broll & Huey, 2015).

When schools and law enforcement are not willing to get involved in preventing the malicious behavior of students, it can cause a vacuum. An unregulated area where if not monitored, could get out of hand. Parents play a big role in how their kids communicate online. They should be the third party to law enforcement and to schools by monitoring what their children do online to prevent them from becoming a victim or a bully.

Security

Gilmour (2014) used the analogy that if the real world was a street, and it was split down the middle, one half of the street would be the cyber world and the other half would be the real world; thus, the police need to be able to patrol both sides of the street. People are the ones who control computers and manage what they do; therefore, humans must be incorporated into the susceptibility of computers being vulnerable to an attack because humans are able to be manipulated (Conteh & Royer, 2016). Conteh and Royer (2016) further explain that humans have emotions that override commitment to logic that is where they make the computer vulnerable; humans' susceptibility makes the computer vulnerable. A computer does not have these vulnerabilities—they are programed to work in a linear fashion not susceptible to human emotions.

People who are trying to get personal information from others will send emails to victims to update their personal account information on various websites, or any information that can help the person gain information about the intended victim. When the person replies, it exploits the gullibility in people, when the person replies to the message thinking it was a legitimate inquiry (Kandpal & Singh, 2013). The criminals that

use these tricks to get information are preying on the imperfections that make us human. One little slip up by the user and the whole computer can be corrupted without them knowing.

Conventional law enforcement prevention tactics do not work well in the cyberspace (Ngo & Jaishankar, 2017). Ngo and Jaishankar (2017) recommend that law enforcement agencies collaborate with agencies within their country, and other countries, to combat the offenses that occur in cyberspace. They also recommend law enforcement work with software companies to produce products that inhibit criminals from committing identity theft on unsuspecting people. The development of security software is a paramount component to prevent cybercrimes from being committed. Informing people about scams and how to protect themselves from inquiring criminals would prevent people from becoming victims.

Policy Implications

Laws that are more effective to deter people from engaging in online illicit behavior need to be created and heavily enforced. A cybercrime division under the executive branch should be created to handle investigating and apprehending these criminals. If it is more likely you will be caught by the authorities when engaging in these crimes and a swift punishment is to follow, then there will be less people using this medium to conduct illegal activities.

The agency should have trained agents who are proficient in the information technology sphere of law enforcement, who are well versed in computer systems and processes. Agents will be recruited like any other law enforcement agency recruits and hires for their agency through advertising and will be filtered out based on the competence of the individuals best fit for the position. This agency will only be

operational if there is a need for its services. If it is successful in suppressing criminal behavior, and criminal acts are reduced to a manageable level where local and federal agencies can handle the workload then the proposed agencies services will be obsolete and therefore disbanded.

The agency will be funded through the taxes collected by the government and by federal grants from the government of the United States. The average American citizen may oppose this, but they need to consider that this is worth the money, due to an imposing threat to this country. The lawmakers must be persuaded to create this agency because of its great importance. A way to show the legitimacy of this agency would be to demonstrate the amount of money that could be saved, and the number of people who are victimized by cybercrime every year. The government could save money by detaining criminals who are defrauding the state, and strengthen the economic infrastructure, because companies will not have to allocate resources to deal with fraudulent claims.

It is important that there be a specialized law enforcement agency dedicated to monitoring the cybersphere, and other parts of the internet that are not necessarily known to regular law enforcement agents. Other agencies are spread too thin because of having to monitor multiple mediums with incredible amounts of data and traffic. It is too much of a workload for so many agencies, already doing multiple jobs and following countless cases. It would take the burden off many agencies, making them more effective. They would not have to assign resources to the cybersphere, and they would be able to focus on the other aspects of crime.

This new agency would solely focus on the internet and computer crimes. Being dedicated to only one realm would make

their work easier, and more efficient. The agents would not necessarily be officers, which could give opportunities to more qualified applicants who might have been disqualified as police officers or other law enforcement agencies, due to physical agility standards or certain health problems.

Success will be measured on whether the number of cybercrimes decreases over a span of five to ten years, or until there are no more funds to keep it running. It will be considered successful when the number of crimes committed over the internet has significantly decreased, and people's lives and livelihoods are saved because of this policy's implementation and the creation of this new agency to combat cybercrime.

Conclusion

Technology plays a big part in most people's lives in this modern era of technology evolution. Computers that once took up large rooms now have been reduced to handheld smartphones that enable people to stay connected with each other. The ability for people to easily connect with one another is what has led to the ability of criminals to abuse technology for their personal gain.

In conclusion, these are a few examples of the many different types of cybercrimes; they are not newly invented crimes, but crimes that are being committed in a new realm. Law enforcement needs to keep up with technology to be effective against these crimes. Technology advances rapidly and it is constantly changing, therefore law enforcement should be constantly adapting to new ways crimes are being committed.

References

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction*, *109*(5), 774-783.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology, 8*(1): 1-20.

Broll, R., & Huey, L. (2015). "Just being mean to somebody isn't a police matter": Police perspectives on policing cyberbullying. *Journal of School Violence, 14*(2), 155-176.

Conteh, N. Y., & Royer, M. D. (2016). The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer (IJC), 20*(1), 1-12.

Diamond, B., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology, 9*(1), 24.

Donner, C. M. (2016). The gender gap and cybercrime: An examination of college students' online offending. *Victims & Offenders, 11*(4), 556-577.

Gilmour, S. (2014). Policing crime and terrorism in cyberspace: An overview. *European Review of Organized Crime, 1*(1), 143-159.

Kandpal, V., & Singh, R. K. (2013). Latest face of cybercrime and its prevention In India. *International Journal of Basic and Applied Sciences, 2*(4), 150-156.

Kerr, O. S., & Murphy, S. D. (2017). Government hacking to light the dark web: What risks to international relations and international law. *Stanford Law Review Online*, 70, 58-69.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2014). Exploration of the cyberbullying victim/offender overlap by sex. *American Journal of Criminal Justice, 39*(3), 538-548.

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367.

Mazowita, B., & Vézina, M. (2014). Police-reported cybercrime in Canada, 2012. *Juristat: Canadian Centre for Justice Statistics, 34*(1), 1-24.

McCusker, R. (2006). Transnational organized cybercrime: distinguishing threat from reality. *Crime, Law and Social Change, 46*(4-5), 257-273.

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the international journal of cyber criminology: A research agenda to advance the scholarship on cybercrime. *International Journal of Cyber Criminology, 11*(1), 1-9.

Ophardt, J. A. (2010). Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duke Law and Technology Review, 9*, 26-54.

Brandon McDaniel transferred to San Jose State University with an associate's degree in Criminal Justice in the fall of 2015. He will be graduating with a bachelor's degree in Justice Studies by the fall of 2018. Brandon aspires to pursue a career in law enforcement. He is most interested in technology and its applicability in criminology. In his spare time, Brandon can be found riding around on one of his many motorcycles. If he is not riding to work or school, he is riding in the dirt for fun.