York University Criminological Review, 2016
Vol. 1, 67-85

THE ORGANIZATION OF CYBER CRIME

Cameron Penny

ABSTRACT

In efforts to dissect and describe the various forms of crime organized over computers and cyber-networks, the present paper follows McIntosh's (as cited in Sheptycki, 2014b) study of the 'organization of crime', to likewise develop a discourse on the 'organization of cybercrime'. Specifically, the paper describes the organization of piracy, hacking, terrorism, and cryptomarkets, revealing the varying motivations and goals of parties involved. Profit oriented or idealistic, ephemeral or long lasting, aptitude based or simplistic, the descriptions of the various organizational aspects are intended to provoke academic inquiry that succeeds in weakening descriptions of cybercrime as a uniformly organized activity. The author concludes by offering recommendations based in the organizational contexts of cybercrime to guide policy makers in developing more comprehensible solutions to cyber threats. Particularly, these recommendations surround surveillance, problem definitions, and technical expertise.

Keywords: *cyber-crime, organization of crime, McIntosh, description, policing*

Cameron Penny graduated from York University in 2016 with a double major bachelor of arts in Criminology and Sociology. Cameron has decided to continue his academic career at the University of Essex in England where he will pursue a master's degree in Sociology.

Published by the Criminological Studies Review Initiative in Toronto, Ontario.
ISSN 2371-6258
http://csri.journals.yorku.ca

INTRODUCTION

"Computer crime", "cyber-crime", and "technocrime" are labels created to describe the modern criminal activities of the information age (See Broadhurst, 2006; McCusker, 2006; and Leman-Langlois, 2008). Though describing similar activities, these labels belie nuances of meaning, leaving academics unsure of how to analyze this subject without conflating terms (McCusker, 2006). Questions of definition surround the newness of criminal endeavours online, their relation to regulatory controls, national borders, and the broader socio-political environment. Significantly, McCusker (2006) questions the popular adoption of "organized crime" rhetoric to describe cyber-crime, a point further elucidated by a litany of other criminologists (Choo & Smith, 2007; Hutchings, 2014; Lusthaus, 2013). Remaining sceptical of any alleged links between "cybercrime" and "organized crime", it is worthwhile to utilize McIntosh's (1975, as cited in Sheptycki, 2014) method of analyzing the organization of crime, to synthesize a discourse on the 'organization of cyber-crime'. Her analytical perspective is useful as it seeks to "describe criminal organization in terms of relations within the wider social structure" rather than examining the criminal groups in a social vacuum (p. xxv). Likewise, this analysis explores sociologically the ways the organization of criminal activity online reflects the varying aspects of cyber-crimes and the social environment that supports them. This study specifically focuses on cryptomarkets, hacking, identity theft, cyber-wars, "hacktivism", and piracy, labels commonly discussed under terms like cyber-crime or technocrime. Though this is by no means an exhaustive list of crimes, it provides a starting point for the primary objective of this paper: descriptions that better correspond to the virtual world of crime by appreciating the shades of organizational difference between cyber-crimes. In an attempt to contribute pragmatically to criminological discourse on cyber-crime, this paper subsequently examines cyber surveillance and policing tactics in hopes to equip policy makers with more comprehensible solutions to cyber-crimes.

PIRACY

Possibly the most prevalent cyber-crime, copyright infringement, or 'piracy' as it has been recently termed, is the present paper's first order of business. There have been many well-publicized piracy cases in recent history, not limited to the case of Kim Dotcom's demise[1] (Palmer & Warren, 2013). These cases illustrate a new form of copying data through the internet, however, Palmer and Warren underline that "as far back as the early twentieth century, innovative uses of photographic and cinematographic technologies enabled the unlawful copying and smuggling of banned films across national borders" (p. 106). The modern difference, the authors argue, is that the inherently borderless nature of communications technology has magnified challenges for traditional law

[1]Kim Dotcom, creator of MegaUpload, an information sharing website, was prosecuted by US authorities on charges of copyright infringement, among others. His website allowed users to upload and download any content, which also included illegal material. His case is especially notable because of the military like seizures that took place at his home in New Zealand.

enforcement to track copyright violators and the corresponding economic costs of their actions. Estimating these costs, Yar (2004) cites movie industry representatives who state the financial cost of these infringements approximate 3 billion USD in lost profits. Additionally, some research suggests a 6.5-8.5% increase in revenue for the movie industry was directly proportionate to MegaUpload's demise (Danaher & Smith, 2013). However, as Yar emphasizes, these outrageous economic costs as described by the media producers, are, "to put it mildly, open to methodological challenge" (p. 689). Therefore, though there may be a real economic cost of copyright infringement, it becomes difficult to quantify these costs because of the politics of generating the statistics, as well as the inability to track the scale of copyright infringement online.

How then is this site of criminal exploitation in the cyber world organized? Breaking the organization down, there are three parties primary to piracy: the facilitating organization (e.g., MegaUpload.com), the individual who downloads illegal data onto their personal computers, and the individual who replicates and distributes illegal content through the facilitating website. The majority of participants are downloaders of illegal content, while a minority are uploaders. In the past, the users engaging in either downloading or uploading have been regarded as one in the same, sharing similar values to hackers (Holt & Copes, 2010). With this link in mind, research has concluded that uploaders/downloaders do not to act as loners, but share collegial and fluid relationships with each other that reinforce their criminal activities (Meyer, 1989, Holt & Copes, 2010). Possible explanations for this link include the historical inaccessibility of illegal goods online for those without extensive technical expertise. However, since 1995 the accessibility of illegal goods online for those with non-technical aptitudes has widened. Consequently, there is at once more individuals able to engage in piracy, and less reason for collaboration (Holt & Copes, 2010). Therefore, further research should look at differentiating these two roles in the contemporary piracy experience, identifying the varying motivations between uploaders and downloaders.

Seeking to explain the motivations of downloaders and uploaders, Higgins, Fell, and Wilson (2006) have produced research that incorporated theoretical material on self-control and social learning. Though interesting as an individual pathology idea, the research ultimately did not interact with the socio-structural elements of cyber-crime this paper seeks to uncover. A more comprehensive understanding of the individual's engagement in piracy would look beyond the individual's innate characteristics to include other elements such as economic costs, as individuals may be unable to afford the legitimate means of consuming media. Additionally, accessibility may be a key, as inserting a legitimate video disc into a disc player may be more cumbersome, or simply unavailable, compared to using a free online video streaming service. Or, following the crowd, the individual may make sense of his/her actions by comparing piracy to jaywalking, as in everyone does it. Lastly, individuals may engage in piracy for ideological ends. Researchers have studied groups who contribute to the production of free software and have concluded that they do so to create a Utopian society of sharing free software, and a better, freer humanity (Baytiyeh & Pfaffman, 2010; Holt & Copes, 2010). Similarly, users and contributors to piracy sharing websites may do so for similar utopian dreams of a share-free universe. Though requiring further empirical evidence, these preceding motivations offer a glimpse into the supporting socio-structural environment that organizes piracy overall. As a consequence, the motivations are more likely to be external to the

individual rather than pathological. This means that the ways in which piracy is socially organized may differ wildly from one individual to the next. For instance, an individual seeking a clip of a movie online that they already own physically might be separated from the true "pirate" label that might be attached to an individual seeking economic gains from illegal downloads. Either way, the motivating elements behind the individual's organization, whether as an uploader or downloader, demands further research for academics to ultimately understand piracy at an individual level.

Contrastingly, considerable scholarship has sought to examine the States' response to MegaUpload, underscoring themes resonating with Charles Tilly (1985) and Fredric Lane (1958) that the state provides the legitimate means of violence to maintain its own motivations (e.g., global economic stature). If the state's economy is under attack by domestic and foreign citizens, it becomes the state's mandate to protect the economy by maintaining the legitimate means of media production through law enforcement or otherwise. Illustrating this phenomenon, Yar (2005) acknowledges the larger overarching system of control that constructed copyright infringement as a criminal infraction, symbolically labelled as a "pirate" and placed alongside "real crimes". What the etymology of "internet piracy" reveals is that interest groups have had a marked influence on law and enforcement strategies by conducting investigations and presenting them to authorities, lobbying for stricter laws/punishment and the inclusion of the language of piracy in law. These investigations liken the replication of copyrighted material to gangs of mariners looting local trade routes demands tough approaches to "violent offenders". These laws produce high profile cases, epitomized in the case of Kim Dotcom, which demonstrates the extent state authorities will go to reduce the copyright infringement practices affecting their economy.

To describe briefly, Kim Dotcom, a citizen of New Zealand and founder of MegaUpload, had his house raided by 76 heavily armed officers in early 2012. There was no evidence to suggest Dotcom was armed or dangerous. Adding to the drama, helicopter and canine teams were also brought in. Raids were simultaneously conducted at various satellite server locations across the globe. What followed was an almost year long wait for New Zealand to extradite Dotcom to the States, while nearly all of his assets were frozen. Palmer and Warren (2013) used court documents to identify a myriad of privacy infractions by the enforcement agencies, including the search and seizure of all his servers. This research illustrates the means by which the police pursued Dotcom was through surveillance strategies were not always legal or backed by significant evidence. Returning to Fredric Lane (1958), this explicit use of violent (and illegal) tactics for a global policing initiative reveal how the police as an institution, like a protection racket, serve the interests of their clients (i.e., corporations and economy) to support their existence. In this case, Dotcom was a client that did not have protection from the state's hidden interest groups (i.e., the media industry) and thus was subject to the state's punishments. These themes will be revisited in the following sections discussing policing and enforcement strategies. Before concluding this section, it is worth noting that in many widely-distributed publications Dotcom was presented as a martyr for citizen's privacy and the scope of policing powers worldwide. He is now hailed as an international celebrity and has met with officials worldwide to discuss issues of surveillance and privacy (Palmer & Warren, 2013). This effect, given the state's response to Dotcom, emphasizes the fine line of criminality that surrounds copyright infringement online.

CRYPTO-MARKETS

Unlike the ambiguity of piracy, crypto-markets and trading forums are among the quintessential cyber-crimes because they are "the most visible and documented form of cybercriminal organization", and they illustrate the extent to which criminals are financially motivated entrepreneurs (Lusthaus, 2013, p. 54). Allowing individuals to move their illicit business off the streets (i.e., drugs, arms, threats of violence), the online marketplaces have produced a potentially safer environment for business while simultaneously creating a market for the vanguard entrepreneurs selling computer viruses, credit card information, and other "cyber" products. To access these markets safely, users (buyers and sellers) utilize The Onion Router (TOR). This is an application and network that works by routing an offender's internet connection to three 'nodes' that disassociate the target location (i.e., Crypto-market website) from the origin point (i.e., User's IP address[2]). Though it was compromised by a U.S. law enforcement agency in the past, TOR is now considered to be impenetrable; however, news in the media suggests both university researchers and law enforcement agencies have discovered new means of de-anonymizing the internet within the last year (Adhikari, 2014; Hill, 2015). The currency of these markets is based on Bitcoins, an unregulated "crypto-currency" that has seen major spikes and decreases in value (Bitcoincharts.com, 2016), but is considered the industry standard. Essentially then, these markets facilitate the buying and selling of illegal commodities (e.g.., drugs), or items that could be otherwise used for illegal ends (e.g., computer viruses), via anonymous connections and transactions spanning the globe. Ultimately, the anonymous nature of both payment and access to these markets produces an almost entirely protected illegal market.

There exists a major difference between activities organized on these crypto-markets. On one hand, crypto-markets have been coined an "eBay for Drugs" (Aldridge & Decary-Hetu, 2014, Barratt, 2012). The quintessential example of this form of crypto-market, Silk Road (existing from 2011-2013), was comprised of various listings of drugs and other illegal goods. The buying and selling of illicit drugs and other commodities like weapons or hitman services through these markets are very prevalent, amounting to an estimated $480 million USD for drugs alone. The benefits of this online organization include the increased operational safety, number of potential customers, as well as the greater variety of quality and quantity of various drugs (Barratt, 2014). On the other hand, recent studies suggest a trend towards hacker oriented markets, increasingly focused on the selling of computer viruses or other technological means to victimize others financially over the internet (Lusthaus, 2013). Because the present paper's goal is to move beyond the analysis of market commodities that have a direct relation to the physical world, the following discussion examines the ways computer crimes are organized online; thus, this paper analyzes virtual crimes in a virtual world. These analyses survey four central actors: the buyer, seller, administrator, and the internet hosting provider.

To start, there is the buyer, sometimes known as the "mule", who makes transactions with

[2]An IP address is a string of numbers that is associated with an internet network or computer device (Beal, "IP address - Internet Protocol (IP) address")

a stolen credit card or operates a purchased virus to retrieve more stolen credit card data. The buyer ultimately retrieves a direct profit from their actions. These individuals need no degree of expertise in disseminating viruses or performing transactions, as the seller often provides an easy "how-to" file. In one case, an individual shipped out programmed fake debit card machines to his/her buyers to make retrieval easier (Lusthaus, 2013). The accessibility of both illicit products and the information around them is supported by Hutching's (2014) research interviews with law enforcement and offenders. Officers stated that, "If you go online to an IRC[3] channel and look at online fraud, there's a myriad of people you can ask, exchange ideas and information and tools and, it's all there for you to get involved," while another admitted that sellers can, "send you complete instructions […] and they'll just talk them through on how to set up" (p. 14). Besides the increased frequency of offences, a consequence of the accessibility of this technical information is that the offending buyers are not forced to work with others to commit their offences (McCusker, 2006). In other words, without a need for further organization, buyers can engage in illicit activities without any support. There are cases, however, where partnerships did exist for a variety of purposes including decreasing the individual costs of viruses on crypto-markets and the probability of being detected by law enforcement (p. 15). It appears then that buyers are individually and economically oriented, and though they do not need to work in groups, they occasionally will cooperate to reach the financial goals of all members. Though the products and information are accessible, in order to avoid being "ripped" (p. 7), the buyers rely on a seller's "reputation points" to gauge their reliability. Similar to Mafia groups, trust becomes a central element to market transactions (Lusthaus, 2013). Those sellers who have a higher number of reputation points are regarded as being more trustworthy, which encourages more sales of their products. Buyers run a higher risk of getting caught, but because of the borderless nature of these markets, buyers are often not prosecuted because of jurisdictional barriers (Hutchings, 2014). Ultimately, the buyers are the simplest of the roles, relying on preexisting networks of sellers to provide them with viruses made by expert coders, or credit card information so that they can cash out stolen currencies in the real world. However, the buyers are entirely dependent on the other actors of the crypto-markets to pursue these ends, which makes the following actor's roles indispensable to the consistency of the markets.

Tightly linked with the buyers, sellers are the second major actor within these markets. They are the creators of computer viruses and collectors of the credit card information. These individuals are highly specialized, not only at producing these illicit products but also in their ability to recruit buyers or mules to complete the riskier processes of cashing out (Lusthaus, 2013). They often work with other sellers to develop these products, as there are few individuals who can produce these specialized strings of code themselves (Dion, 2001; Holt, 2013). Their specific activities outside the market will be discussed in the section on hacking. In the case of financial fraud, they may retrieve the credit information initially through traditional or digital means: that is, through

[3]Internet Relay Channel - allows group and private communication between users on the internet.
[4]Phishing - "to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one" ("Phishing", n.d.)

purse snatching or computer engineering. Computer engineering, simply being phishing[4], or other fraudulent websites appearing to be legitimate, trick the user into entering sensitive information. These means are preferable as the victim may not know until much later that they have been victimized. This ensures that the value of the seller's product is maintained, and the buyers receive a reliable product.

The third yet often overlooked actors are the market owners and administrators themselves. Though not necessarily engaging in any buying or selling of the services offered on their websites, they maintain a rank that allows them the ability to "ban" malicious users from the market, a level of virtual violence that draws a parallel to Gambetta's (1991) key elements of the Mafia's reputation for violence. Their publicly understood power to remove individuals from the market, like a reputation for violence, may deter users from scamming others. In addition, Lusthaus draws a secondary parallel to Varese (as cited in Lusthaus, 2013), noting that the higher ranked individuals are able to "provide a degree of third-party enforcement over illicit transactions online" (p. 55). The final relation of these actors to mafia types is the owner's goal to create a monopoly on illicit sales online, sometimes through 'violence'. This was well illustrated in one instance when hacker 'Iceman' took down other crypto-markets and unified them into one. He said that his motive was "...security. Convenience. Increase quality and decrease the noise. Bringing order to a mess…" (Lusthaus, 2013, p. 56). In this case, Iceman had effectively removed his competition by "attacking" the competition's websites' servers with a DDoS[5] attack, while consolidating buyer and seller user data into his crypto-market. This tactic gave Iceman a monopoly over all crypto-markets; therefore, when one examines the upper administration of crypto-markets, it is evident that there are many similarities between traditional Mafia-like organized crime and crypto-markets because of the administrator's prerogative to enforce rules, maintain a reputation for violence, and dominate marketplaces.

The final actors are beyond any single individual within the market, but fundamentally supports the market's existence. They are the hosting organizations that provide secure and reliable servers outside the jurisdiction of the transactions made in the crypto-markets. Offered by organizations such as the Russian Business Network, their services are known as 'bulletproof hosting'. These providers have also demonstrated an ability to engage as protection rackets by launching Distributed Denial of Service (DDoS) attacks against illicit websites and then offering protection for figures such as $2000 a month (Lusthaus, 2013). Ultimately, Lusthaus admits there is little data on these services, yet their "ostensible operations serve as a useful discussion point" (p. 58). It is crucial to consider the ways in which these hosting companies make use of law enforcement's jurisdictional barriers to protect users of crypto-markets. Without these boundaries, the hosting companies would have no role in the underground markets online, and the other actors would have to rely on potentially problematic digital tools such as TOR to remain anonymous. Thus, the institutions of law enforcement have created this criminal opportunity by allowing for cross-

[5]DDoS – Denial of service, or DoS, attacks, involve overloading a website or computer system so that legitimate access is blocked. When using botnets this is known as a distributed denial of service, or DDoS, attack (Grabosky, 2007, as cited in Hutchings, 2014)

jurisdictional barriers in the enforcement of law globally.

Zooming out to the wider picture, crypto-markets present a network-like appearance, allowing individuals to buy, sell, and converse with other like-minded individuals. Their existence is ephemeral, as illustrated many times over with the destruction of markets such as Silk Road. There is a clear division of labour, especially evinced by the mules who 'cash out' the profits of sellers. There are ranks and a level of governance over transactions. Put simply, they are a business. They are profit rather than ideologically driven.

HACKING

If we are to liken crypto-markets to businesses, hacking can be regarded as an art, and the art of hacking is as dynamic as the technology that produces it. Hacking originally began in the 1950s and 1960s with individuals interested in computers and technology, and it has developed to include "phone phreaking", security hacking, and other activities (Loper, 2001). Steinmetz (2014) contends that hacking today is more than simply scamming unsuspecting computer users. It is a "transgressive craft" that uses programming to reach particular ends. These ends, whether taking down a website or unlocking a phone, are not important in themselves, as the focus of the hackers is more on the process than the outcome. Acts of hacking are not criminal in themselves, although they have often been represented as criminal conduct. A small percentage of individuals do engage in hacking with malicious intents rather than pure curiosity. These activities include logging user's keystrokes, hacking passwords, infecting computers with viruses, gaining backdoor access to systems, and spam. The public dependency on the systems that facilitate these activities only increases potential harm (McCusker, 2006). It is this small percentage of hackers who exploit the public's dependency on digital tools that this discussion surrounds.

Because the activities hackers are engaged in require only a computer and one's own technical aptitude, the hacker has been represented as a "lonely dateless loser pecking away at the basement computer" (McCafferty, 2004). McCafferty, a writer for the Web Host Interview Review (WHIR), explains that this representation is no longer accurate. The continually greater amounts to steal (because of the increases in transactions online and accessibility of sensitive financial information) are being exploited by a "new breed of smarter criminals" who work together with clearly defined roles. The idea of a well-organized underground is mirrored in official statements produced by organizations such as the Public Safety Canada's Cyber-Crime Strategy. According to former minister Vic Toews, hackers exist as highly organized groups who set out to victimize Canadians (Public Safety Canada, 2010). These assertions have not been empirically supported, as research has discovered in the past that hackers tend to work alone, or in fluid partnerships with other hackers. (Meyer, 1989). Rather, these statements reflect the state's ignorance of the academic literature on hacker organization. When hackers do associate, Meyer states the computer underground is more of "a social organization of colleagues" (1989, p. 65). As a collegial group, hackers are able to offer each other a support network to enhance their own technical aptitude and boast their achievements. Further, McCusker (2006) argues that "such an affiliation is not essential for the pursuit of a criminal career, as it is for members of real-world gangs" (p. 264).

Thus, there is no evidence to support assertions that the criminal underground is expanding, or becoming more organized, and any claims to that effect are not supported by empirical evidence. They simply reflect the transference of traditional organized crime language to the virtual world.

Examining hackers as individuals, Nikitina (2012) suggests hackers, unlike the ugly suggestion of "hacking" as something rough and uncoordinated, are more "tricksters" who are able to use technical knowledge and cunning techniques to complete an objective. This technical aptitude, McCusker (2006) argues, is the only reason that hackers would collaborate. It is unclear as to whether these autonomous youths and tricksters play a large role in the financial victimization of individuals. It is important to note that hackers are qualitatively different from other non-computer financial crimes in that they represent particular demographics of individuals who have an aptitude for technological assaults and a personality like a "trickster", where hackers take pride in their work. As Steinman (2014) underlines, there is a clear sub-culture of hackers which reproduces values of privacy, perceptions towards government institutions, commitment, and a common phenomenological experience. Ultimately, it appears that hackers do form loose networks, forming think tanks to hone their technical skills, while also developing an internal code of values and goals. These values and goals may be especially present in groups with ideological motivations.

These groups that engage in "hacktivism" are excellent examples of ideologically-oriented groups. According to Choo & Smith's (2007) typology, there are two specific motivations of ideologically motivated criminals: terror, and perceived inequalities (e.g. ecological, political, or ethical equality). The former will be discussed in later considerations of terrorist groups' involvement in the virtual world, but for now it is enough to focus on the activists that take their protests online. These groups typically protest through Denial of Service (DoS) attacks, targeting the antagonist individual or group's virtual image (i.e., corporate website). They also have been known to release confidential information in the name of freedom of information (Hutchings, 2014). The most popular hacktivist group is "Anonymous", which is reported to have started in 2008 on the image board 4chan. It has taken a central position in international hacktivist goals. Anonymous spokespersons define themselves by writing,

> We [Anonymous] just happen to be a group of people on the Internet who need—just kind of an outlet to do as we wish, that we wouldn't be able to do in regular society. ... That's more or less the point of it. Do as you wish. ... There's a common phrase: 'we are doing it for the lulz[6].' (Schultz, 2008).

Perhaps this philosophical statement reflects their early initiatives in 2008, which included many different pranks online; however, it is possible to identify a new transformation of their activities. Recently, after the terrorist attack on Charlie Hebdo in France, Anonymous has allegedly "declared war" on al-Qaeda and linked terrorists. This announcement preceded attacks on many of the extremist groups' websites, which resulted in many of those sites being removed from the internet.

[6]In other words, for the fun of it.

Anonymous, like most hacker groups, does not have a centralized leadership. This assertion is directly supported by a website associated with Anonymous. Instead, they describe themselves as "an Internet gathering" with "a very loose and decentralized command structure that operates on ideas rather than directives" (Kelly, 2012). They have been noted to circulate on Internet Relay Channels (IRC's) to plan their activities. Unlike hacker groups, anonymous participants are not necessarily hackers. The media shows images of protestors wearing masks and marches on the streets, yet also reports on the actual hacking done under the name Anonymous. Whether there is a central leadership of hackers within the non-hacker whole is inconclusive, yet certainly demands further research. Very little scholarly research has been done on "Anonymous" and similar groups. When they are studied, it is unclear if the subject of analysis is the group or a particular individual within it.

Crucially, unlike the sellers in crypto-markets, there appears to be a disjuncture between the hackers and the vast plethora of individuals simply capable of committing financial crimes over the internet. The hackers described in the previous section, the loosely grouped individuals who share many normative elements (such as goals, purposes, and values), appear to be more of tradesmen than scoundrels or tightly organized maleficent groups. It would be useful for future scholarly research to elucidate the sub-cultures of hackers by utilizing ethnographic methodologies in a manner similar to Steinman's (2014) research on hacker communities worldwide. This may prove useful in creating a more succinct understanding of the underlying motivations and goals of hackers, and their qualitative differences from actors found in other forms of cyber-crime.

CYBERWARS

Gagnon (2008) predicts that the future of the internet, which invariably includes the (re) militarization[7] of the web, involves "committing cyber-crimes for cybersecurity purposes becom[ing] the norm" (p. 63). These "crimes", Gagnon explains, reflect a blurring of the terms cyber-crime and cyberwar in the interests of national security. This has been demonstrated through the FBI's inclusion of a cyber criminal in their top ten most-wanted list, as well as the US government's decision to include cyber concerns in the mandate of the U.S. Department of Defense. The USA's activities of cyber warfare are ultimately unknown, yet reported leaks describe their methods as "highly efficient", holding the potential to shorten wars (p. 53). Similarly, beyond the USA, China is described as an emerging threat. It wields cyber weapons that could "easily cripple the national infrastructures of its potential enemies" (Tkacik, 2008, as cited in Gagnon, 2008). In fact, China has already been reported to have downloaded ten to twenty terabytes of data from the United States' NIPRNet (Non-classified Internet Protocol Router Network) (Gagnon, 2008). It is suspected that China will soon surpass the USA's cyber dominance if it has not already.

As these activities between state actors inherently exist outside any single nation's rule of

[5]When the internet was created, it was a military asset for rapid communications through international networks. Later, it became an educational, then public resource. Gagnon's (re)militarization refers to the drift from public to military control over the internet.

law, it becomes difficult to discuss these acts by the U.S., China, or others as "criminal" at all. Instead, it is easier to offer insights into the harms of these maneuvers, although little is known about them. Primarily, the harms include the perceived provoking of inter-state war. For instance, when Estonia moved a statue that signified part of Russia's history, major government sites went offline. Though this was later reported to have been a mere coincidence, Estonian officials had already launched a counter cyber-attack on Russian government computers, assuming Russia's motivations (Gagnon, 2008). Had this perceived attack on Estonia and the real attack on Russia been received poorly, it is possible that a "real" war may have broken out. In addition to international harms, we can examine the domestic harms of cyber warfare methods. Domestically, China wields these weapons to control citizens' use of the internet, with particular interests in protecting the security of the nation. Gagnon notes that there are 30,000 Chinese government workers systematically reading emails, blogs, bulletin boards, internet forums and chatrooms, attempting to ensure Chinese (approximately 10 million) users are protected against "offensive content". China, the state, effectively becomes a protection racket in its ability to monopolize citizens' use of the internet while providing privacy protection. Gagnon states that this protection of privacy is paradoxically secured in the Chinese organization of cyberspace.

Because the state is the primary actor in these cyber-wars, an analysis of state structures and influences is necessary to produce an accurate depiction of how cyber-war is organized. For one, levels of centralization are quite similar across the two major cyber powers, China and the USA. Just as Gagnon highlights, the various anti-cyber-crime actors within the U.S., not limited to the department of Homeland Security, Federal Bureau of Investigation (FBI), or the Central Intelligence Agency (CIA), China also has a multitude of state authorities involved in internet regulation and protection. These agencies are continually evolving into more national defense-oriented organizations that focus on cyber-crime as a threat to the sovereignty of the nation-state, rather than viewing cyber-crime as an issue of criminality between citizens. A second similarity is the secrecy and invisibility of the activities state agents engage in, such as those that may have shortened the Kosovo war (Knight 1999, as cited in Gagnon, 2008). Little is known about these activities, and, unless counter surveillance measures are employed by the public or an information leak is made, research remains inconclusive. Differences between states, Gagnon hints, are not in their activities, which are increasingly becoming idiosyncratic, but in their ideological foundations. In other words, though the methods of cyber-war are essentially the same, the underlying goals and motivations differ from nation to nation.

TERRORISM

Eugene Kaspersky, the founder of Kaspersky Lab, contends that "cyber-terrorism" is the correct term when one discusses computer "attacks" online. He states that "with today's attacks, you are clueless about who did it or when they will strike again" (Shamah, 2012). Kaspersky's rhetoric of "terror" online conflates all the aforementioned forms of cyber-crime with the very ideologically different real-world terrorist groups such as al-Qaeda or ISIS. These real-world terrorist groups are the second of Choo and Smith's (2007) "ideologically motivated criminal groups". They

use computers and computer networks to target "critical infrastructure such as electricity, water, communications, air traffic control and financial systems" (Hutchings, 2014, p. 4). It is crucial to identify this unique difference between Kasperksky and Choo & Smith's use of the term "terror", as it may help to dispel misrepresentations of all cyber-crimes as terrorist like, or vice versa. This next section examines these uniquely terrorist organizations.

Citing Theoharry and Rollins (2011), Hutchings asserts that there is no evidence to support the claim that the real-world terrorist groups currently engage in hacking activities to reach their ends. However, various reports in the media suggest the opposite. In one such report 'spy chief' Andrew Parker stated that the imminent threats of an ISIS-associated group, Cyber Caliphate, were very real (Graham-Harrison, 2015). If these reports are accurate, the terrorist organizations worldwide may be taking a new appreciation to hacking, especially in cases where their target is geographically distant. Ultimately, these groups' role in interrupting critical infrastructure remain uncertain (Broadhurst, 2006). Hacking aside, Hutchings (2014) highlights how real-world terrorist organizations already engage in other forms of financially motivated cyber-crime to fund their ideologically inspired actions in the real world. Additionally, terrorist organizations use the internet to plan their attacks, recruit members, distribute propaganda, and communicate with organizational nodes. The same media source confirms these conclusions, highlighting the ways these groups are actively recruiting new hackers to strengthen their operations (Graham-Harrison, 2015). Moving forward, it is predicted, and perhaps even expected, that the ideologically motivated real-world terrorist groups will converge with financially motivated groups to produce a very different threat than imagined in Choo and Smith's (2007) typology (McCusker, 2006). At that point we will no longer be able to discuss real-world organized crime groups and real-world terrorist groups as separate entities, but codependent organizations.

POLICING

Reviewing the litany of actors, from individuals to nation states, it becomes evident that crime engaged in and through computers and cyber networks is organized in very different manners to pursue very different ends. When one is providing recommendations to reduce these activities, it is crucial to appreciate these fundamental variances. The following section seeks to pursue these considerations by examining three sites of proposed development: surveillance, definitions, and technical expertise.

Surveillance

With fraudsters, hackers, and otherwise criminal individuals working online, a higher level of surveillance may prove useful. In the past, it has been instrumental in removing previous markets such as Silk Road, by allowing law enforcement access to the usernames, emails, and other sensitive information of this market's users (Hutchings, 2014). Barricades to achieving this type of surveillance nowadays include the alleged impenetrability of the TOR network and citizen's rights. Recently, a new barricade to surveillance has appeared, and that is private corporations' willingness to aid law enforcement. In a groundbreaking case in the USA, the FBI took Apple Inc. to court asserting

that Apple was not complying with law enforcement, by refusing to unlock a deceased terrorist's iPhone. Apple, who publicly opened a discussion on this, stated, that the FBI asked them to create something "too dangerous […] they have asked us to build a backdoor to the iPhone" (Cook, 2016). Since then, the FBI has opened the phone with the aid from an unnamed private entity, effectively short-circuiting the legal case at hand, at least for now (Barrett & Wakabayashi, 2016). This case is significant because it shows how private sector organizations hold the power to disrupt law enforcement operations. If other organizations such as internet service providers also continue down the same road as Apple in the name of "data security", it may be impossible for law enforcement to ever capture individuals engaging in crypto-markets, hacking, terrorism, or otherwise, without circumventing civil rights. Therefore, it may be in the interests of law to increase surveillance abilities of law enforcement, and decrease private organization's ability to interfere with investigations.

However, as Palmer and Warren (2013) identify, higher levels of surveillance can signify large scale violations of civil rights, something a trusted state agency cannot risk, lest the public lose confidence in the state's ability to govern. The case of Kim Dotcom, among others, illustrates just how far law enforcement will go to pursue criminals despite the rights of its citizens. Thus, it would be ill-advised to allow law enforcement agencies greater surveillance without the appropriate safeguards. Instead, following Mann (as cited in Manning, 2008), the public might be better if they had access to "sousveillance" of these powerful groups. Sousveillance operates in exactly the same ways as the police by allowing citizens to see where the authorities are looking. Potentially, this could ensure that when powerful authorities do violate individual's rights, they do so on a public stage, forcing them to anticipate the public's reactions. In many respects, these contradicting concerns of surveillance and civil rights are reconciled in David Brin's (2008) comment that an environment in which both privacy and surveillance are privileged "will not be a convenient or anonymous world. Privacy may have to be redefined much closer to home. There will be a lot of noise. But we will not drown under a rising tide of uncontrolled technology" (Brin, 2008, p. 26).

Definitions

The second area of development, definitions, calls on the political influences that contribute to the production of definitions of cyber-crime being privileged over others. In regards to illegal downloading, Yar (2004) identifies the media producers as major contributors to the US government's denunciation of piracy. Yar discusses a piracy case in Malaysia where a minister blamed the media producers for a marked increase in individuals downloading illegal content after prices of foreign media increased. Rather than punish the consumers of this media, or the distributors, perhaps the government should focus on negotiations with media to reduce the cost of movies; therefore, increasing legitimate sales. It is possible that the media producer may lose profits, just as they are now from illegal downloading, but it would allow a compromise between profits and the unnecessary violent persecution of those such as Kim Dotcom.

Another problematic definition held by law enforcement is the perceived prevalence of traditional Mafia-like organized crime in all areas of cyber-crime. Though these preceding discussions have not devoted a significant amount of time to discussing the relations between cyber-crime and traditional organized crime groups, McCusker (2006), Lusthaus (2013), and Hutchings (2014) all

conclude that, in Lusthaus' words, "we should not necessarily expect exact replicas of traditional criminal organization online" (p. 59). Yet, as highlighted by Canada's stance on cyber security, there is an alleged threat by organized groups to Canadians online (Public Safety Canada, 2010). The disjuncture reflects what Broadhurst (2011) identifies as one of the main challenges to policing cyber-crime; namely, "catching up" to the various forms of cyber-crime, especially as technological changes affect its organization. Rather, following the descriptions provided in the present paper, law enforcement might approach cyber-crimes in a new light, appreciative of the unique organizational elements.

Technical Expertise

This idea of catching up is especially apparent when one discusses the technical aptitude of law enforcement combating cyber-crime. If the criminal's reputation is based on his/her technical aptitude (McCusker, 2006), police organizations might flourish by keeping up with their criminal counterpart's technical aptitudes. This includes understanding how criminals avoid detection from the law, and it means keeping up with technological advancements and utilizing and developing them when possible. It means going beyond law enforcement's current notions of cyber-crime as "high-tech crime", presupposing criminals as being essentially the same as in the physical realm, and acknowledging that cyber-crime is qualitatively different than other forms of crime. Further, it may mean more partnerships with private organizations to develop this technology for law enforcement. With a burgeoning virtual world of cyber-crime, it becomes crucial for law enforcement to update themselves consistently and thoroughly with the technical aspects of cyber-crime.

CONCLUSION

"Computer crimes", "cyber-crime", and "technocrime" are labels created to describe the new criminal activities of the information age. Though often conflated in academia, government, and elsewhere, the previous discussions have demonstrated that the crimes that fall under these terms can be organized quite disparately. To recall, there are differences based on motivation, technical aptitude, length of participation, among others. Consequently, uniform depictions of cyber criminals or cyber-crimes, such as is offered by government and academic literature, are no longer relevant. Instead, spring boarding from the aforementioned introductions to the different forms of cyber-crime, academics are encouraged to produce scholarship that appreciates the shades of organizational difference between cyber-crimes. The positive effects of this progression, besides providing more concise depictions of the subject for academics, include the potential this discourse would have for policymakers and law enforcement. Able to develop tactics specific to the various forms of organization, officials may stand a better chance of combating and preventing crime rather than presupposing a uniform organizational unit of cyber-crime. Beyond law enforcement, criminal courts may stand a better chance of reducing recidivism by assessing the underlying motivations of individual's engagement and provide appropriate sentences. Further still, by acknowledging the plethora of participants in activities such as piracy, as well as their relatively harmless motivations, crime and the law itself may be redefined. Ultimately, the implications of academics developing a

discourse on the organization of crime transcend pure scholarly discussions and may have a direct effect on how so-called cyber-crimes are responded to by all facets of the criminal justice system.

WORKS CITED

Adhikari, R. (2014, August 1). Tor Has Been Breached - What Now? Retrieved June 12, 2016, from http://www.technewsworld.com/story/80834.html

Aldridge, J., & Decary-Hetu, D. (2014). Not an 'eBay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *SSRN Electronic Journal*. doi:10.2139/ssrn.2436643

Barratt, M. J. (2012), Silk Road: eBay for Drugs. *Addiction*, 107(1), p. 683. doi: 10.1111/j.1360-0443.2011.03709.x

Barrett, D., & Wakabayashi, D. (2016, March 28). FBI Opens San Bernardino Shooter's iPhone; U.S. Drops Demand on Apple. Retrieved April 07, 2016, from http://www.wsj.com/articles/fbi-unlocks-terrorists-iphone-without-apples-help-1459202353

Baytiyeh, H., & Pfaffman, J. (2010). Open Source Software: A community of altruists. *Computers in Human Behavior*, *26*(6), pp. 1345-1354. doi:10.1016/j.chb.2010.04.008

Beal, B. V. (n.d.). IP address - Internet Protocol (IP) address. Retrieved September 15, 2016, from http://www.webopedia.com/TERM/I/IP_address.html

Bitcoincharts.com (2016). "Bitcoin Charts." Retrieved April 8th 2016 from http://bitcoincharts.com/charts/bitstampUSD#rg2920ztgSzm1g10zm2g25zv

Brin, David. (2008). Crime and lawfulness in the age of all-seeing techno-humanity. In S. Leman-Langlois (Ed.), *Technocrime: Technology, crime, and social control* (pp. 243-246). Devon, UK: Willan Publishing.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management, 29*(2), pp. 408-433. doi:10.1108/13639510610684674

Choo, K & Smith, R. (2007). Criminal Exploitation of Online Systems by Organised Crime Groups. *Asian Criminology*. 3, pp. 37-59. Print.

Cook, T. (2016, February 16). Customer Letter - Apple. Retrieved April 06, 2016, from http://www.apple.com/customer-letter/

Danaher, B., & Smith, M. D. (2013). Gone in 60 Seconds: The Impact of the MegaUpload Shutdown on Movie Sales. *SSRN Electronic Journal*. doi:10.2139/ssrn.2229349

Dion, D. (2001). "Script Kiddies and Packet Monkeys – The New Generation of Hackers." Retrieved on April 8th 2016 from https://www.giac.org/paper/gsec/395/script-kiddies-packet-monkeys-generation-hackers/101009

Gagnon, B. (2008). Cyberwars and Cybercrimes. In S. Leman-Langlois (Ed.), *Technocrime: Technology, crime, and social control* (pp. 46-65). Devon, UK: Willan Publishing.

Gambetta, D. (1991). 'In the beginning was the Word…' The symbols of the mafia. *European Journal of Sociology, 32*(1), pp. 53-65. doi:10.1017/s0003975600006147

Graham-Harrison, E. (2015, April 12). Could Isis' 'cyber caliphate' unleash a deadly attack on key targets? Retrieved April 06, 2016, from http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated Self-Control theory and social learning theory using structural equation modeling. *Criminal Justice Studies, 19*(1), pp. 3-22. doi:10.1080/14786010600615934

Hill, K. (2015, November 30). The Attack That Broke the Dark Web-and How Tor Plans to Fix It. Retrieved June 12, 2016, from http://fusion.net/story/238742/tor-carnegie-mellon-attack/

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165-177. doi:http://dx.doi.org/10.1177/0894439312452998

Holt, T. J., & Copes, H. (2010). Transferring Subcultural Knowledge On-Line: Practices and Beliefs of Persistent Digital Pirates. *Deviant Behavior, 31*(7), 625-654. doi:10.1080/01639620903231548

Hutchings (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime Law and Social Change, 62*, pp. 1-20. DOI 10.1007/s10611-014-9520-z

Kelly, Brian (2012). "Investing in a Centralized Cybersecurity Infrastructure: Why 'Hacktivism' can and should influence cybersecurity reform" (PDF). *Boston University Law Review, 92* (5): pp. 1663–1710. Print.

Lane, F. (1958). Economic Consequences of Organized Violence. *Journal of Economic History,* 18, pp. 401-417. Print.

Leman-Langlois, S. (2008). Introduction: Technocrime. In S. Leman-Langlois (Ed.), *Technocrime: Technology, crime, and social control* (pp. 1-13). Devon, UK: Willan Publishing.

Loper, D. K. (2001). The Criminology of Computer Hackers: A Qualitative and Quantitative Analysis

(Doctoral dissertation, Michigan State U, 2000). *Dissertation Abstracts International: The Humanities and Social Sciences, 61*(8).

Lusthaus, J. (2013). How Organised is Organised Cybercrime? *Global Crime, 14*(1), pp. 52-60. 10.1080/17440572.2012.759508

Manning, P. (2008). A View of Surveillance. In S. Leman-Langlois (Ed.), T*echnocrime: Technology, crime, and social control* (pp. 209-242). Devon, UK: Willan Publishing.

McCafferty, D. (2004). Organized Cyber Crime - Web Host Industry Review. Retrieved April 06, 2016, from http://www.thewhir.com/organized-cyber-crime

McCusker, R. (2006). Transnational Organised Cyber Crime: Distinguishing threat from reality. *Law and Social Change*, *46*(4-5), pp. 257-273. doi:10.1007/s10611-007-9059-3

Meyer, Gordon R. (1989). The Social Organization of the Computer Underground. Diss. Northern Illinois U, *G2 Meyer Dot Com*. Web. 6 Apr. 2016.

Nikitina, S. (2012), Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture. *The Journal of Popular Culture, 4*5, pp. 133–152. doi: 10.1111/j.1540-5931.2011.00915.x

Palmer, D., & Warren, I. J. (2013). Global Policing and the Case of Kim Dotcom. *International Journal for Crime, Justice and Social Democracy, 2*(3). doi:10.5204/ijcjsd.v2i3.105

Phishing. (n.d.). Dictionary.com Unabridged. Retrieved June 12, 2016 from Dictionary.com website http://www.dictionary.com/browse/phishing

Public Safety Canada. (2010). *Canada's Cyber Security Strategy for a stronger and more prosperous Canada*. [Ottawa]: Vic Toews.

Shamah, D. (2012, June 6). Latest viruses could mean 'end of world as we know it,' says man who discovered Flame. Retrieved April 06, 2016, from http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/

Sheptycki, J. (2014). Introduction. In J. Sheptycki (Ed.), Transnational Organized Crime, Volume 1 (pp. Vii-Xx). Los Angeles: SAGE.

Schultz, D. (2008, March 1). Community Organization with Digital Tools. Retrieved April 07, 2016, from http://mediashift.org/2008/03/community-organization-with-digital-tools005/

Steinmetz, K.F., (2015). Craft (y) ness An Ethnographic Study of Hacking. *British Journal of Criminology*,

55(1), pp. 125-145. doi:10.1093/bjc/azu061

Theohary, C.A. and Rollins, J., (2011). Terrorist Use of the Internet: Information operations in cyberspace. *Congressional Research Services*. Pp. 1-16. Retrieved April 8th 2016 from https://www.fas.org/sgp/crs/terror/R41674.pdf

Tilly, C. (1985). War Making and State Making as Organized Crime. In P. B. Evans, D. Rueschemeer, and T. Skocpol (eds), *Bringing the State Back In* pp. 169-191. doi:10.1017/cbo9780511628283.008

Yar, M. (2005). The Global 'Epidemic' of Movie 'Piracy': Crime-wave or Social Construction? *Media, Culture & Society, 27*(5), pp. 677-696. doi:10.1177/0163443705055723