A NEW STATE OF ORGANIZED CRIME: AN ANALYSIS OF ORGANIZED CYBERCRIME NETWORKS, ACTIVITIES, AND EMERGING THREATS

Davina Shanti, Simon Fraser University

Abstract

Organized crime is often associated with traditional criminal groups, such as the mafia or outlaw motorcycle gangs; however, new research suggests that cybercrime is emerging as a new branch of organized crime. This paper is focused on the changing nature of organized crime and the factors that influence this shift, particularly in the online space. It will address the question: Can the law identify cybercrime as organized crime? The results of this paper are informed by an in-depth analysis of peer-reviewed articles from Canada, the United States (US), and Europe. This paper concludes that cybercrime groups are structured and operate similarly to traditional organized crime groups and should, therefore, be classified as a part of traditional organized crime; however, cybercrime groups are capable of conducting illicit activities that surpass those typically associated with traditional organized crime. This shift suggests that these groups may represent a larger threat creating a new challenge for law enforcement agencies.

Keywords: Organized crime, cybercrime

Cybercrime groups have established themselves as structured enterprises operating within a larger network and may be identified as a branch of traditional organized crime groups. The expansion and intricate nature of cybercrime activities has arguably led to a growth in networks and profit for online groups. Crypto markets have evolved to facilitate the commission of complex cybercrimes and are dominated by organized criminals with progressive skills and knowledge (Tiirmaa-Klaar, 2013, p. 8). This paper discusses two points: First, it looks at how organized cybercrime compares to traditional organized crime. Second, it considers how the changing nature of organized crime may require an alternative outlook in how we identify organized crime groups and their activities to include a cyber perspective.

Organized Cyber Crime and Traditional Organized Crime

Many types of cybercrime can be related to some form of organized criminal activity. Cyber-attacks and hacking are cheap ways of gaining strategic

advantages or illicit income with very few resources (Tiirmaa-Klaar, 2013, p. 22). It can be argued that financial motivation is what drives the illicit activities conducted by cybercrime groups (Broadhurst et al., 2014, p. 3; Lusthaus, 2013, p. 53; Leukfeldt et al., 2017, p. 289). As shown in Table 1 (see below), the types of illicit activities conducted by organized cybercrime groups tend to be unique to operating in an online space, and arguably, are more complex than activities associated with traditional organized crime groups. Activities of cybercrime groups include hacking, distributing malware, stealing personal data or private records, piracy, phishing, botnets, carding, distributing illicit drugs, and online sexual offending (Broadhurst et al., 2014, p. 5-6). The most common form of cybercrime is spreading malicious programs, or malware, to hijack personal computers or poorly protected computers of companies. These methods are used to collect information, steal personal data, distribute spam, and launch denial of service attacks (Tiirmaa-Klaar, 2013, p. 2-3; Leukfeldt et al., 2017, p. 289; Graff, 2017).

Profit is made from infecting computers and websites, selling personal data, or stealing banking information or credit card data. These attacks grow in complexity as more computers are affected and more data is stolen for profit. One way this is done is through botnets. A botnet is a network of infected computers that is directed to distribute spam, denial of service attacks, and malware (Graff, 2017). Botnets have been used to attack financial services, such as banking institutions, and over the years they have grown more sophisticated in order to bypass detection (Tiirmaa-Klaar, 2013, p. 8). Lastly, hackers may sell bugs for profit as they are worth a lot of money and pinpoint the vulnerabilities in operating systems (Grossman, 2014). A software bug is an error or mistake in a computer program or operating system that causes the program to behave unexpectedly. If a hacker finds a bug, they can use it to steal data and information, or they can sell it on the black market for others to do the same (Grossman, 2014). Cyber criminals profit off of collecting personal data and information and using it to steal money or selling it for more profit.

Table 1

Illicit Activity Variations Amongst Traditional Organized Crime Groups & Organized Cybercrime Groups

Traditional Organized Crime Groups vs. Organized Cybercrime Groups		
	Similarities	Differences
Type of Illicit Activities	Trafficking illicit drugs, trafficking weapons, human trafficking, fraud, embezzlement, theft, robbery, racketeering, and money laundering.	Hacking, malware, ransomware, botnets, email spam, carding, skimming, identity fraud, phishing, distributing child exploitation materials, creating and distributing disinformation, distributing propaganda and recruiting for extremist groups, and cyber espionage.

However, not all groups are capable of committing these crimes. Some activities are executed by groups that have a stricter hierarchy, similar to traditional organized crime groups, such as crime families (Broadhurst et al., 2014, p. 6). This may be because certain crimes are more sophisticated and require a group of skilled, knowledgeable, trustworthy individuals. It is the core members of groups who are often the ones who coordinate attacks and provide direction; therefore, they are likely to have the most knowledge and skill (Leukfeldt et al., 2017, p. 291). Similar to traditional organized crime groups, organized cybercrime groups vary in their structure and chain of command. For example, groups that operate as hubs have a central command structure that is hierarchical, and there is often a leader or cluster of core members and associates who operate outside the core group (Broadhurst et al., 2014, p. 5).

However, Lusthaus (2013) argues that cybercrime still lacks formal hierarchy, and individuals work together to share information and collaborate, but not delegate orders (p. 57). Those groups who may have some hierarchical structure lack the ability to properly govern activities within the darknet market (Lusthaus, 2013, p. 57). This may be true in cases where groups are formed loosely with novice hackers, but it cannot be applied generally to all cybercrime groups and online spaces. In addition, it may be imprecise to apply a traditional outlook on what organized crime should be without addressing the context and changing

nature of online crime. For example, forums are marketplaces where illicit goods and services are advertised and sold (Broadhurst et al., 2014, p. 7; Lusthaus, 2013, p. 54). These marketplaces have a clearly defined hierarchy with an administrator, moderators, and various user groups whose status and privileges vary. Similar to a traditional organized crime group, members who prove to be trustworthy and provide good services are given more opportunity and can move up in rank (Leukfeldt et al., 2017, p. 294; Lusthaus, 2013, p. 54). Although some cyber criminals protect these marketplace forums, it can be argued that they provide a similar service as the mafia but are in no way a mafia-type group. It is challenging to govern an online forum where users are anonymous and virtual punishment is less effective than physical punishment (Lusthaus, 2013, p. 56).

Networks amongst cyber criminals are similar to those of traditional organized crime. Individuals, or core members, operating within the same cybercrime groups, are usually family or close friends and tend to be located within the same geographic proximity (Leukfeldt et al., 2017, p. 291-293; Broadhurst et al., 2014, p. 3). These offline social contacts are important for networking in the online space, but this does not mean that connections cannot be made online as well. Networking also occurs through online discussion forums and chat rooms rather than face-to-face meetings. However, massive network growth is based on the established long-term trust between individuals (Leukfeldt et al., 2017, p. 293). Online criminals are capable of linking up and carrying out attacks together, in fact, the online space arguably makes it easier for connections to be made. For example, a hacker who went by the name Slavic led a small trusted circle of cyber criminals to spread malware throughout financial institutions. Once employees' computers were affected by malware, logins were stolen, and Slavic's group was able to move stolen money into various bank accounts. He used money mules to open up new accounts at different financial institutions and withdraw the funds (Graff, 2017). The network that Slavic has created mimics that of a traditional organized crime network. There is a structure in place that enables the flow of knowledge and resources, and monetary gain. Even amongst cyber criminals, networks are important to establish relationships to ensure the operational aspect of the business is maintained.

Changing Nature of Organized Crime

Cyber criminals are always learning how to improve their attacks and manipulate the systems that are already in place. The complexity of these crimes increases as hackers increase their knowledge and skillset and learn to break down new protective measures against cybercrimes. Organized cybercrime networks have shifted their dependency from people to rely on networks of computers, internet

service providers, bank accounts, and digital wallets to facilitate business. The advanced nature in which these crimes are executed suggest a transformation in organized crime. Attacks can now be directed remotely with crimes being committed internationally (Graff, 2017). For example, botnets can be commanded from any location, and hackers may choose to concentrate their attacks within countries that have ineffective cybercrime laws (Tiirmaa-Klaar, 2013, p. 11). This not only represents the transnational nature of cybercrime, but the advancement in the strategic operations of these attacks.

Cryptocurrencies, such as Bitcoin, have become popular services used by hacking groups in money laundering schemes, and have arguably enabled them to efficiently launder their money and effectively evade law enforcement. Bitcoin is a decentralised form of electronic currency. To avoid detection and throw off investigators, cyber criminals make transactions unclear as they create new digital wallets and route funds through mixers to conceal the money trail (Bojarski, 2015, p. 37; Bohme et al., 2015, p. 230). Bitcoin has been able to illegally facilitate money laundering activities by bypassing conventional means of payment and by offering a degree of anonymity to users (Bojarski, 2015, p. 37; Kruisbergen et al., 2019, p. 576). A currency like Bitcoin enables users on the dark web to anonymize their transaction to a certain degree, which in turn may encourage criminal activity, such as money laundering and the buying and selling of illicit goods and services (Kruisbergen et al., 2019, p. 576). The ability to better hide one's identity and money laundering activities may offer an explanation as to why cybercrime has become more attractive to organized crime groups. Operating an illicit business or illicit activities in an online space offers a veil of protection where it may be less easy to be detected by law enforcement. In the most ideal cases, cybercriminal groups are able to operate at a relatively low risk in turn for a high profit simply by obscuring individual identities and paper trails.

Organized cybercrime activities have shifted into state-sponsored cybercrime, where private criminal actors may collaborate with state authorities. For example, the botnet *GameOver Zeus*, created by Evgeniy Bogachev (otherwise known as Slavic), may have been used as a Russian intelligence gathering tool (Graff, 2017). Similarly, the hacker group *PLA Unit 61398* was able to gain access to a US manufacturer's company network and retrieve information on pending negotiations, pricing documents, and other sensitive materials (Broadhurst et al., 2014, p. 15). The operational transition of organized crime groups represents a change in how the law might identify cybercrime activities, but more importantly the element of violence. Lusthaus (2013) argues that violence is a part of

traditional organized crime, but cybercrime groups are not capable of causing physical harm in the same way that the mafia or outlaw motorcycle gangs are (p. 58). Violence is an action punishable by law, and it can be argued that it is part of how organized crime groups are identified. Although these individuals operate their criminal activities in an online space, it does not necessarily mean they are incapable of committing acts of violence (Leukfeldt et al., 2017, p. 294). As shown in Table 2, the effects of violence can be seen in an alternative way that does not only consider kinetic action. Cyber-attacks for espionage and information collection is a form of non-kinetic warfare, where the outcome may be intended to spread propaganda or destabilize democratic nations rather than to have an immediate physical effect (Fallaha, 2017). Therefore, it can be argued that cyberattacks, in the form of hacking, espionage, botnets, malware, and ransomware, may be classified as forms of non-kinetic violence.

Table 2

Use of Violence Amongst Traditional Organized Crime Groups & Organized Cybercrime Groups

Factors	Traditional Organized Crime Groups	Organized Cybercrime Groups
Type of Violence (Kinetic vs. Non-Kinetic)	Kinetic - physical violence involving the use of weapons, or the act of physically assaulting someone.	Non-Kinetic - violence is not physical and does not have a kinetic outcome. Rather, acts of violence can be seen as attacking another person, group, state, business, or organization through nonconventional methods involving cyber-attacks.
Purpose of Violence	To threaten, intimidate, and punish. Meant to cause physical harm or death.	Arguably, the purpose of this form of violence is purely for financial gain. Non-kinetic violence enables groups to commit cybercrimes, conduct attacks, obtain personal or confidential information, and disseminate false information in exchange for money.

SFU LIBRARY DIGITAL PUBLISHING

Use of Weapons	Use of guns, knives, brass knuckles, bear spray, taser and explosives. Body parts, such as hands, can be classified as a weapon as well, if used to cause physical harm or death.	Use of computer and internet as a weapon to conduct illicit activities, and pinpoint vulnerabilities in victims.
Outcome of Violence (Harm Caused)	Physical harm or death.	Personal harm, such as identity theft or fraud. Financial harm which can result from identity theft, carding, skimming, or ransomware. Operational harms, such as obtaining confidential documents or information that may halt business operations. Victims can include an organization, business, or institution. Operational harms may also lead to both financial and personal harms.

The definition of organized crime states that participation must involve three or more persons acting as a collective (Leukfeldt et al., 2017, p. 295; Broadhurst et al., 2014, p. 4; Royal Canadian Mounted Police, 2011). However, this definition may not encompass the organization of a botnet operated by a single offender (Broadhurst et al., 2014, p. 4). It can be argued that a network of malicious software is a form of organized crime as participation may not always involve persons, but computers and software instead. Attackers are able to build peer-to-peer networks of infected computers that are nearly immune to dismantling efforts. For example, if one computer's command server is interrupted, the owner can simply set up a new server and redirect the network to it (Graff, 2017). This may suggest the need for a change in how organized crime networks are identified and understood.

In addition, new organized cybercrime groups continue to emerge on the dark web and take on some of the traditional structural roles in order to regulate and control the distribution of a product or service (Lusthaus, 2013, p. 57). If online marketplaces and forums become defunct, members may try and build a new forum, although the organizational aspect has seemingly disappeared with the takedown of the leader and the website. It can be argued that the reticulate nature

of organized crime groups has allowed for illicit activity and cyberattacks to continue even with the downfall of a leader and the hierarchical structure. A law enforcement strategy of ‘‘taking out the leader’’ does not work on a network which may not need a fixed leader to continue to operate (Strang, 2014, p. 12). These groups may have shifted into an operational use of net-centricity, where individual actors within the network perform as nodes that help facilitate and preserve the purpose of the criminal activity (Meyers, 2019, p. 5; Kelshall, 2018, p. 28). Online communication has enabled groups and networks to be rebuilt and newly constructed so quickly that the fall of a leader or site does not mean that the group is completely dismantled and its activities stop.

Conclusion

Organized cybercrime and traditional organized crime have many similarities in the operational structure, network, and range of involvement in illicit activities. Cybercriminal groups have been able to establish themselves as powerful actors who are not only capable of providing illicit products and services on the dark web but are able to conduct damaging attacks against vital industries and government agencies. They use the dark web to their advantage to protect themselves, their services, and their profits, and are constantly adapting their knowledge and skillset to prolong detection from law enforcement. The degree of sophistication suggests that these cybercrime groups are capable of being highly organized and should be considered to be an organized crime group. However, the way we identify organized cybercrime and its activities represents a challenge. Cybercrime is difficult to combat because, just like traditional organized crime, it occurs simultaneously in many jurisdictions, and attackers are able to change their location to avoid detection. Cyberattacks can take place anywhere in the world and do not have to be commanded by an individual located in the same vicinity as the attack. Furthermore, the nature of cyber threats is continuously evolving and is not limited by physical boundaries or state borders. Therefore, it is important to be able to conceptualize the changing nature of organized crime and its emerging trends to account for the dynamic nature of these groups. Cybercriminals take advantage of the vulnerabilities within law enforcement control strategies and constantly improve their tactics to stay ahead and hidden.

For cybercrime to be fought effectively, it is important to ensure that combatting cybercrime is part of a broader national strategy that encourages the cooperation between national law enforcement and security agencies. Elements, such as proper legislation, international law enforcement cooperation, information sharing, and proper crime reporting should be implemented (Tiirmaa-Klaar,

2013, p. 26-35). It is suggested that law enforcement be given more investigative powers and resources to address the seriousness of cybercrime groups (Leukfeldt et al., 2017, p. 297). In order for strategies to actually work, more resources need to be allocated to addressing cybercrimes. Dedicating more people, money, and tools could mean a better understanding of how these groups operate so that law enforcement can keep up with the changing methods of this crime.

References

Bohme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213-238. http://dx.doi.org/10.1257/jep.29.2.213

Bojarski, E. (2015). Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations. *The European Review of Organized Crime, 2*(2), 25-50.

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

Fallaha, S. (August 9, 2017). Non-kinetic warfare: Defence and strategy in political war. *NATO Association*. http://natoassociation.ca/non-kineticwarfare-defense-and-strategy-in-political-war/

Graff, G.M. (2017, March 21). Inside the hunt for Russia's most notorious hacker. *Wired*. https://www.wired.com/2017/03/russian-hacker-spy-botnet/

Grossman, L. (2014, July 10). The code war: The internet is a battlefield, the prize is your information, and bugs are weapons. *Time*. https://time.com/magazine/us/2972309/july-21st-2014-vol-184-no-3-u-s/

Kelshall, C. M. (2018). Chapter 2: Violent transnational social movements. In C. M. Kelshall & V. Dittmar (Eds.), *Accidental Power: How Non-State Actors Hijacked Legitimacy and Re-Shaped the International System* (pp. 24-39). Burnaby, BC: Simon Fraser University Library

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime & Justice*, *42*(5), 569–581. https://doi.org/10.1080/0735648X.2019.1692420

Leukfeldt, E.R., Lavorgna, A., & Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal of*

Criminal Policy and Research, *23*, 287-300. DOI: 10.1007/s10610-016-9332-z

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52-60. http://dx.doi.org/10.1080/17440572.2012.759508

Meyers, S. (2019). Is there a gap in Canada's hate crime laws? The identification of soft violence as a tool for current right-wing extremist social movements. *The Journal of Intelligence, Conflict, and Warfare*, *2*(2), 1-11.

Royal Canadian Mounted Police. (2011). *What is organized crime?* Royal Canadian Mounted Police. https://www.rcmp-grc.gc.ca/soc-cgco/whatquoi-eng.htm

Strang, S.J. (2014) Network Analysis in Criminal Intelligence. In: Masys A. (eds) *Networks and Network Analysis for Defence and Security*. Lecture Notes in Social Networks (pp.1-26). Springer, Cham.

Tiirmaa-Klaar, H. (2013). Chapter 1: Botnets, cybercrime and national security. In Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E., & Martini, P. *Botnets* (pp. 1-38). Springer.

This work is licensed under a Creative Commons Attribution-Non-Commercial-No Derivatives 4.0 International License.

© (DAVINA SHANTI, 2020)

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University, Volume 3, Issue 1.

Available from: https://jicw.org/