TECHNOLOGY AS A TOOL FOR TRANSNATIONAL ORGANIZED CRIME: NETWORKING AND MONEY LAUNDERING

Gurpreet Tung, Canadian Association for Security and Intelligence Studies – Vancouver

Abstract

Using technology to commit crimes is becoming much more prevalent. The internet has provided organized criminal entities anonymity and accessibility to criminal networks across the world to expand their illicit businesses. Technology is allowing for different organizations to co-exist and assist one another to achieve their goals. Organized crime entities are not only utilizing cyberspaces to communicate with networks across the globe but are also utilizing these spaces to aid in money laundering. Money laundering processes have begun to move online to better obscure assets in relation to criminal activity. Therefore, technology is creating a more dynamic and complex world to combat organized crime.

Introduction

The word 'transnational' refers to the ability to go beyond borders, boundaries, jurisdictions, and nations. Technology has extended boundaries and reach for several businesses, including organized crime entities (Kassab & Rosen, 2019; Kruisbergen et al., 2019; Saito, 2021). Transnational organized crime operates globally with various markets in different countries (Kassab & Rosen, 2019). An example of a common business venture among organized crime is the trafficking of drugs. Like legitimate businesses, organized crime groups also make decisions based on the larger costs/benefits analysis model (Kassab & Rosen, 2019; Kruisbergen et al., 2017). The high demand for drugs, such as cocaine and amphetamines, tends to result in more benefits than costs to criminal organizations, making it more appealing among criminal organizations (Kassab & Rosen, 2019; Kruisbergen et al., 2017).

Organized crime groups also consider several parts of the supply chain, such as production, supply, distribution, and transportation, which are vital components to meet demand (Kassab & Rosen, 2019). Each of these phases in the supply chain are supported by international markets in which countries around the world contribute to the supply, production, distribution, and/or transportation of a variety of drugs; the production and distribution of drugs is a well-known global business as different countries specialize in the production of different drugs (Kassab & Rosen, 2019). Thus, to build networks and reach different markets in different countries, there must be a line of communication, and technology has

become a tool used by organized crime to transcend boundaries and connect with foreign associates (Kassab & Rosen, 2019; Kruisbergen et al., 2019; Saito, 2021).

Transnational Organized Crime: Technological Benefits

Technology has created new secure channels of communication, for example, encrypted phone messaging applications (apps) such as Sky ECC and EncroChat (Saito, 2021). Encryption is not a difficult technique to learn, which makes it an appealing option for anyone, specifically criminals (McDonald, 2021). End-to-end encryption apps provide a protected channel of communication for organized crime entities to network with international partners by concealing the identities and locations of those involved (Saito, 2021). Sky ECC was an end-to-end encrypted messaging app developed by Sky Global, a Canadian company, to offer anonymous, secure, non-traceable communication to its users (Saito, 2021). Furthermore, Sky ECC was discovered to be a common app used for communication among international drug trafficking organizations (DTOs) (Saito, 2021). Eventually, Sky Global was indicted for providing a means to facilitate illegal products and no longer exists since it was shut down by law enforcement (Saito, 2021). One way in which Sky ECC guaranteed anonymity was by using cryptocurrencies during exchanges and in money laundering processes (Saito, 2021). Therefore, this demonstrates that technology is a powerful aid that organized crime entities use not only to communicate with local networks but also with international networks. For example, the production of opium in Afghanistan and the production and/or supply of chemicals to produce synthetic drugs from or in China and India are later supplied and distributed in other parts of the world (Kassab & Rosen, 2019).

Thus, this demonstrates the transnational effect of drugs and organized crime because it impacts not only one country but several others as the product moves through the supply chain. Currently, with the development of new technology, organized crime entities have expanded their networks internationally; accessibility to the internet has allowed these entities to create business relationships and communicate with one another around the world. These relationships with different groups contribute to different elements of the supply chain, which contributes to monetary gain for each of the entities involved (Edwards & Gill, 2002; Kassab & Rosen, 2019).

The online realm has altered communication among organized crime entities and their business partners. All criminals now have the option of utilizing cyberspaces through the dark web or encrypted apps to communicate anonymously (Kassab & Rosen, 2019; Saito, 2021). There have been several

studies that have shown that the use of the internet has created more efficient measures in trafficking illicit substances and products, which only contribute to the expansion of business opportunities for organized crime groups (Kruisbergen et al., 2019). For example, potential buyers/consumers have increased largely because of the global reach technology has created for all users and distributors (Kassab & Rosen, 2019). The internet will continue to evolve providing new means to communicate and connect with populations around the world, and therefore, criminals will continuously adapt and create new possibilities to expand their businesses, and most importantly, their financial gain (Kassab & Rosen, 2019). However, that is not to say that all organized crime activities and communications have become completely virtual or digitized, it is instead a combination of both. Traditional aspects still exist, such as production and even distribution at the lower, local levels such as a drug dealer selling to their regular customer on the same street corner (Kruisbergen et al., 2019).

Likewise, similar to how trust plays an important role in legal business relationships, organized crime also values a level of trust built between all parties involved (Kruisbergen et al., 2019). One can even argue that trust is even much more important between criminal entities because of the risk and repercussions they face if they are caught. Once the cohesion is built, cyberspaces have allowed for more accessible and protected communication for criminal organizations to run their business operations with others, such as potential consumers and transporters of their products (Kassab & Rosen, 2019; Kruisbergen et al., 2019). Additionally, organized crime groups no longer have to carry several burner phones to communicate a drop; instead, they can use an online space with networks such as TOR, which can protect their identity (Kassab & Rosen, 2019). Further, the internet has not only provided means for secure communication for criminal organizations, but it has also developed ways in which criminals can conceal and protect their assets and take care of their profits by introducing opportunities to launder money through online domains (Kruisbergen et al., 2019).

Money as the Motivation

Motivations differ for different criminals, and it is motivation that drives criminals to act the way they do. Possible motivators of crime are driven by the need of power, political landscape, and emotion, yet the primary motivator for most crimes appears to be money. The monetary profits criminals make can drive their criminality, especially for organized crime entities (Kruisbergen et al., 2019). Organized crime groups are often involved in the trafficking of illicit products to fund their organization and themselves (Kassab & Rosen, 2019).

Specifically, the monetary gain within drug trafficking is around $320 billion, and those that profit are the organized crime entities, while the ones that are negatively affected are societies, in particular the economic and the health care infrastructures (Kassab & Rosen, 2019). Profits made by the illegal ventures of organized crime groups will likely be 'cleaned'/laundered so that criminals can use it legally (Kassab & Rosen, 2019). Living in a society where organized crime led entities have direct involvement in societal profits is not only a threat to the economy, but also the political regime and society as a whole (Kassab & Rosen, 2019; Kruisbergen et al., 2017). The threat of money laundering within organized crime entities has now expanded thanks to the possibilities the internet has created for these groups to extend their illegal businesses, such as drug trafficking. This in turn, increases profits for the organization and money laundering becomes a much more significant factor in the world of organized crime.

Organized Crime: Money Laundering

Money laundering is a significant aspect of organized crime; if the money cannot be spent, then what is the point of committing crimes? Similar to every other business, organized crime must make money to fund all parts of their illegal activity within the supply chain. As mentioned above, the first part of having a business is to ensure that the business that an organization has committed to is profitable. Therefore, drug trafficking, like other illicit markets, such as human trafficking and the trafficking of weapons, is a profitable business because of the demand (Kassab & Rosen, 2019). So, when money is flowing for the organization, it must be laundered for it to be legitimatized before it is spent 'cautiously' by criminals and their organizations (Kruisbergen et al., 2019). That is why the 'follow the money' or the 'paper trail' concepts, in which the money leads to the apprehension or criminals and organizations, are significant when analyzing organized crime (Kruisbergen et al., 2019).

However, money laundering can be a difficult process for law enforcement to combat. Organized crime groups will invest in legal companies to run their money through, so that it is cleaned and does not raise red flags within law enforcement (Barone & Masciandaro, 2011; Kruisbergen et al., 2019). Suspicions raised by law enforcement can be minimized if organized crime entities invest in larger markets that are legal and in high demand because it 'makes sense' for that market to be conveying that large amount of money (Barone & Masciandaro, 2011; Kruisbergen et al., 2019). In addition to investing in legal markets, organized crime may utilize complex measures to diversify their "money laundering procedures" (Barone & Masciandaro, 2011, p. 119) using

multiple layers to conceal the true origins of the money. The nexus between organized crime groups and terrorist groups have also been found among money laundering investigations. For example, a money laundering process that began in the 70s was uncovered between the 'Ndrangheta and the Provisional Irish Republican Army (PIRA) (Jupp & Garrod, 2019). It involved a complex process of funneling money into offshore accounts and properties, which was later reinvested into criminal activities (Jupp & Garrod, 2019). Moreover, following the 'paper trail' of an organized crime entity in today's everchanging world has become even more complex than before due to the level of anonymity and encryption that technology now offers.

Money Laundering Online

Cryptocurrency is changing the way in which transnational organized crime groups launder their funds and assets (Venezuela Investigative Unit, 2021). Cryptocurrency is a digital currency that uses a blockchain to provide a decentralized, peer-to-peer, and end-to-end encryption channel, which allows for more secure and anonymous transactions (Huberman et al., 2021). These types of transactions can be highly beneficial, especially for criminals. There are cryptocurrencies that provides greater encryption and protection from being traced such as Zerocoin and Darkcoin (Tropina, 2016). Nevertheless, criminal entities may choose to still be involved in traditional methods of money laundering because they are satisfied with the success they have had. However, organized crime groups have been shown to incorporate online activity in different parts of the money laundering process (Kruisbergen et al., 2019; Tropina, 2016; Venezuela Investigative Unit, 2021). For example, there is evidence of organized crime groups using banking malware to conceal expensive and luxurious purchases, as well as during the exchange of cryptocurrency into physical cash (Kruisbergen et al., 2019; Tropina, 2016). Additionally, organized crime entities have shown interest in purchasing bitcoins to better protect their assets (Kruisbergen et al., 2019). Bitcoins assist in masking profits and investments that criminals make into companies by disguising the origins of the profit (Kruisbergen et al., 2019). Further, bitcoin ATMs may be used to deposit large amounts of cash without revealing the origin and identity of the funds (Venezuela Investigative Unit, 2021). Therefore, providing a viable option for organized crime to launder large amounts of money 'safely' online.

However, the amount of known criminal organizations that are indeed utilizing cryptocurrency appears to be small for now (Kruisbergen et al., 2019; Tropina, 2016). Chainanalysis, which is a software company for bitcoin, reports that just over one percent of cryptocurrency is used for money laundering, while also

admitting that there may be ‘rogue’ transactions linked to criminal entities, but they go undetected, and therefore, unaccounted for (Venezuela Investigative Unit, 2021). Thus, organized crime may find it more beneficial for their growth to move online. Yet, the lack of knowledge and market regarding cryptocurrencies may be a deterrent for some criminals (Kruisbergen et al., 2019). In one case, Kruisbergen et al. (2019) found that a drug dealer exchanged their bitcoins for cash in person in a public space with Wi-Fi to ensure the correct amount of money was transferred over. Another reason why criminals may still opt into exchanging products and funds in person is because some online forums that exchange bitcoins for cash require personal information (Kruisbergen et al., 2019). Some criminals may not want to provide their personal information, and instead prefer the exchange to occur in person to better conceal their identity. This is interesting, because most online forums provide anonymity and a secure environment for communication among users. Additionally, criminal organizations must have ‘physical’ monetary profits to be able to acquire any cryptocurrency, but physical cash will continue to exist as long as it remains their favorable payment option in the ‘real world’.

Organized crime groups tend to invest their money in the real estate market in the country they reside in, and this has been discovered in traditional money laundering processes and money laundering online (Kruisbergen et al., 2019). However, differences, such as encryption embedded into multiple layers was found during the concealment of the investments in order to derail law enforcement and investigations (Kruisbergen et al., 2019). Cryptocurrencies allow criminal organizations to anonymize their transactions and identities (Kruisbergen et al., 2019; Tropina, 2016). Therefore, the main difference of online and offline criminality lies in the anonymity of criminal activities; it can be difficult to locate traces of an identity that can be linked back to an individual or an entire organization through the dark web. Nevertheless, organized crime entities have shown that they prefer traditional means of money laundering processes but adopting cryptocurrency and moving operations online are becoming feasible options (Kruisbergen et al., 2019).

Combatting Transnational Organized Crime Online

Law enforcement agencies study members of specific organized crime entities because they provide useful insights into their organizations. This information is important when tracking their criminal activities and the profits they make from their involvement in criminal activities to trace money laundering processes. Money laundering should be a primary target to dismantle organized crime groups, but it is a difficult process to prove in court as evidence can be difficult

to collect since transnational organized crime crosses borders, which means different laws are in effect (Kruisbergen et al., 2017; Tropina, 2016). Nonetheless, for law enforcement agencies it is important to remember that these organizations are unlikely to operate completely online. If the options are not available to investigate online, they will be once the operation becomes offline. For example, when they exchange cryptocurrency back into physical cash since cash is still the favorable payment option considering that the bitcoin market is possibly unstable. However, waiting for the exchange to happen does introduce the risk of the money already being laundered and difficult to trace back.

Thus, cyberspaces create challenges for law enforcement, but also provide evidence for investigations through open-source intelligence (OSINT) platforms (McDonald, 2021). One of the challenges discussed by law enforcement when combatting criminals online is decryption (McDonald, 2021). Decryption is a potential obstacle that law enforcement may have to overcome prior to gaining access to devices, documents, etc. (McDonald, 2021). Law enforcement must be certain during decryption that laws and policies are followed to ensure privacy laws are not breached, whereas criminals do not have to worry about these laws or policies (McDonald, 2021). Overall, as organized criminal entities become more sophisticated, understanding cyberspaces and how they can be utilized is one of the first steps in combatting organized crime because eventually, whether it be DTOs communicating with one another or laundering monetary profits made from illegal businesses, they are likely to be operating online (Kassab & Rosen, 2019; Kruisbergen et al., 2019).

Conclusion

Technology has shifted the world in many ways, both positive and negative. For criminals, it has been a significant addition to their involvement in illegal activities as they are constantly evolving. That is not to say that traditional methods will not remain, but instead they will be infused with online methods. With the primary motivation for organized crime being financial gain, technology provides a means to communicate globally with protection and ease to assist in illegal businesses (Kassab & Rosen, 2019). Transnational organized crime entities benefit from the illicit drug market, and evidence has shown that criminals use online channels to launder money through the purchase of cryptocurrency (Kruisbergen et al., 2019; Tropina, 2016). Therefore, combatting organized crime has now become much more dynamic and complex with the addition of technology. Law enforcement must take into consideration new laws that have been introduced in their country, such as new firearm prohibitions in Canada, and how that will affect the organized crime business and ultimately,

society. They must strategize to combat transnational organized crime online by first, becoming familiar with the processes of how organized crime entities utilize online forums and encrypted apps to conduct their businesses, and then, learn to use them to better understand these cyberspaces to better develop strategic solutions.

References

Barone, R., & Masciandaro, D. (2011). Organized crime, money laundering and legal economy: Theory and simulations. *European Journal of Law and Economics, 32*(1), 115-142. https://doi.org/10.1007/s10657-010-9203-x

Edwards, A., & Gill, P. (2002). Crime as enterprise? The case of "transnational organised crime". *Crime, Law & Social Change, 37*(3), 203-223. https://doi.org/10.1023/A:1015025509582

Huberman, G., Leshno, J., & Moallemi, C. (2021). Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *The Review of Economic Studies.* https://doi.org/10.1093/restud/rdab014

Jupp, J., & Garrod, M. (2019). Legacies of the troubles: The links between organized crime and terrorism in Northern Island. *Studies in Conflict & Terrorism,* 1-40. https://doi.org/10.1080/1057610X.2019.1678878

Kassab, H., & Rosen, J. (2019). General trends in drug and organized crime on a global scale. In H. Kassab & J. Rosen (Eds.), *Illicit markets, organized crime, and global security* (pp. 87-109). Palgrave Macmillan.

Kruisbergen, E. (2017). *Combatting organized crime: A study on undercover policing and the follow-the-money strategy* [Master's thesis, Vrije Universiteit]. ResearchGate.

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

McDonald, D. (2021). Policing in the 21st century. *The Journal of Intelligence, Conflict, and Warfare, 3*(3), 114–116. https://doi.org/10.21810/jicw.v3i3.2769

Saito, H. (2021, April 15). *What criminals plan via encrypted messaging services*. InSight Crime. https://insightcrime.org/news/what-criminals-plan-via-encrypted-messaging-services/

Tropina, T. (2016). The nexus of information technologies and illicit financial flows: Phenomenon and legal challenges. *ERA-Forum, 17*(3), 369-384. https://doi.org/10.1007/s12027-016-0435-2

Venezuela Investigative Unit. (2021, April 7). *Bitcoin cryptocurrency adds to Venezuela money laundering risk*. InSight Crime. https://insightcrime.org/news/bitcoin-cryptocurrency-adds-venezuela-money-laundering-risk/

Author Biography

Gurpreet Tung is the Membership Liaison for the Canadian Association for Security and Intelligence Studies (CASIS) – Vancouver. She has completed an undergraduate bachelor's degree in Criminology and Psychology at Simon Fraser University (SFU) and is currently in the Crime and Intelligence Analysis program at the British Columbia Institute of Technology (BCIT). Her research interest include transnational organized crime entities and money laundering.

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/