Abstract

This research investigates and shows how technology helped to facilitate and to connect three types of transnational crimes. More specifically, cybercrimes, drug trafficking, and money laundering. Moreover, technology has helped to facilitate cybercrimes by basically giving birth to them; without the evolution of technology, we would not have had cybercrimes. When ICTs (Information and communication technology) showed up, people all over the world can now have access to the internet which can make some of them vulnerable to cybercriminals. Examples of cybercrimes can include hacking, Ransomware, Identity theft, phishing emails, Internet Crime Against Children (ICAC), industrial espionage, and fraud.

As for drug trafficking, technology has helped to facilitate this type of cybercrime by basically giving dealers and consumers a safe atmosphere where they can make deals and payments from anywhere in the world without the need of physical appearance which makes them less exposed to getting arrested. Examples of electronic drug trading are the hidden market places in the darknet.

As for money laundering, technology has provided money launderers the ability to establish online offshore companies and banks that have fewer restrictions on money laundering; this method helps criminals to wash their money in countries with no or few laws that prohibit and investigate unknown income sources. Furthermore, technology has provided online banking which gives people the ability to make online transactions; cybercriminals can easily blend their illicit transactions with the illicit ones with less chance of getting noticed.

Other than facilitating those crimes, technology has also helped to connect those three types of crimes. Cybercriminals help drug dealers with coding and providing cyberspace, both cybercriminals and drug traffickers launder their money to have legit unquestionable income.

As for recommended policy implications, nations should keep updating their laws in order to properly prosecute these types of crimes, more education for law enforcement agencies should be implied as well along with more awareness to the public to avoid victimization.

[Keywords] Cybercrime, Drug Trafficking, Money Laundering, Darknet, Transnational Crime

1. Introduction

Everything evolves as times passes. Technology is central to human evolution; it has evolved over thousands of years and will continue to evolve until the end of the world. As technology has evolved, it has enabled the evolution of the world, improving and making life on this planet easier and faster. Whether it is physical technology, technological hardware that can be used as a mechanical instrument (e.g., machines, vehicles, cameras) [1][2], or digital technology information that is coded and programmed into software to work as part of a machine (e.g., artificial intelligence, applications, internet), the evolution of technology has made communication,
business, traveling, security, entertainment, and the majority of human activity significantly more accessible and more efficient.

The evolution of technology has also benefited criminals and evolved the world of crime[3]. As the evolution of technology has transformed the world, crime and criminals have also evolved and transformed in type, methods, complexity, and adaptation to new prevention methods enacted by law enforcement. With the help of technology, traditional crimes can modernize and advance[3].

In addition to benefiting criminals and facilitating crime, technology has also played a role in fighting crime through its use by criminal justice departments. Law enforcement agencies across the globe have utilized technology to maximize security and minimize crime rates[3]. For example, through programs, machines, and other technology, law enforcement agencies have been able to improve their intelligence mechanisms, to scan for explosives and any law-violating items, and to ensure security while minimizing damages caused by criminals.

Although technology is an umbrella term, this research considers the evolution of technology as the independent variable, and specifically information and communication technology (ICT). ICT refers to any technology that helps to produce, store, transmit, communicate and disseminate information in all forms, including voice, text, data, graphics, and video[3]. Examples of ICT include both hardware (machines and devices) and software (e.g., applications, programs, malware).

Information and communication technology largely focus on the Internet. According to Nuth(2008), the Internet is the network of computer networks. At its origin, the Internet was merely a tool of communication to exchange messages between computers. However, with the evolution of technology, the Internet has evolved into the subject (place), object (target), and tool (instrument)[3]. When a computer connects to the Internet, it connects to millions, if not billions, of other computers located across the globe at a low cost[3]. Nuth(2008) argues that there is no such thing as territorial space when it comes to the Internet. In other words, people from all around the world can connect and surf the Internet however they want, with minimum physical restrictions.

Criminals have taken advantage of the Internet. As a tool for international connection, the Internet offers many opportunities for criminals to act upon, and a massive field to roam and practice criminal activity[3]. With the help of this technology, criminals can now communicate, plan, commit, and monitor their criminal acts with reduced risk of capture due to the absence of physical appearance[3][4]. The Internet draws the bridge for criminals to commit their crimes remotely and from the coziness of their desk chair. Nuth(2008) provides a basic example of how an individual or a group of criminals, either experienced or self-taught, can crash the European stock market and cause global chaos for many nations.

As it has helped criminals and crime, the evolution of technology has also helped law enforcement agencies in preventing, reducing, and minimizing the damage of crimes. Nuth(2008) argues that both sides have benefitted from technology. For law enforcement and criminal justice, both physical and digital technologies have been implemented in fighting the battle against crime and criminals. Nuth(2008) provides the example of a basic physical technology that has been implemented in many nations and has worked as a great deterrent for criminals: the installation of closed-circuit television surveillance systems (CCTV) in public or private spaces has helped in reducing crime rates in the United States and the United Kingdom.

Crime technology is an unwanted but unavoidable race[3]. Due to rapid adaptation by criminals and organized crime groups, law enforcement agencies and criminals are racing to surpass each other. Every new invention is followed by a newer one. For example, telephones and mobiles were first invented to communicate. Those devices were soon exposed to evolution and now can record conversations through electromagnetic impulses [3]. The endless cycle of technology evolution will never stop advancing, while criminals and
law enforcement agencies race each other to adapt to the new mechanisms offered by such evolution[3]. However, Nuth(2008) emphasizes how technology can backfire on law enforcement agencies. He explains that when law enforcement agencies adopt new technology to help them fight crime, criminals can study this new technology, develop newer versions, and use it to their benefit to overcome the challenge posed by law enforcement. For example, when law enforcement agencies introduced DNA-testing technology, criminals took that technology and used it in their favor, adopting it to remove their DNA traces from the crime scene, or even replace their DNA with someone else's[3].

Cybercrimes, drug trading, and money laundering are the dependent variables for this research. This study demonstrates how technology can facilitate and connect these three types of transnational crimes. Cybercrimes refer to every crime related to the Internet(e.g., hacking, sabotaging, cyber terrorism, theft, identity theft), while drug trading covers the transition of traditional drug trading to modern and digital drug trading(i.e., via surfing the dark web, which offers the ability for sellers and buyers to browse, communicate, seal deals, and exchange payments). Drug trading also refers to hardware technology that helps drug traders in transporting their drugs with the use of technology(e.g., transporting drugs via drones from point A to point B). This research also demonstrates how technology has introduced more methods for criminals to launder their money(e.g., buying and selling programs’ codes, electronic copies of games or music).

This research fills the gap in understanding the role of technology in the overlap between cybercrimes, drug trading, and money laundering. For example, cybercriminals can create their e-commerce store in the darknet. Darknet is an area of the Internet that is not shown to the public; it has a strong inscription that cannot be accessed with regular browsers. Browsers that provide users access to the darknet include a browser called TOR or the onion router, which was made many years ago by the United States Navy to allow them to encrypt their intelligence sharing with the anonymity it provides[4]. Through its anonymity and encryption, the darknet enables drug traders to make deals via the Internet and make profits that they can launder and wash via purchasing and selling digital goods.

This research also addresses some of the policies that have been implemented over the years to prevent cybercrimes, drug trading, and money laundering using the evolution of technology. It examines why such policy implementations are not working properly in preventing crimes. Also, the research suggests which type of those three crimes is the most serious and why. Finally, this research reviews previous studies regarding how technology can impede transnational crimes by merging it with new policies to fight those three types of transnational crimes and provides recent and historic examples for each variable and policy discussed.

Although the umbrella of transnational crimes covers many different types of crimes, the three types above of crimes were specifically chosen because the variables are logically related. Without the evolution of technology, cybercrimes would not exist, as the Internet is the origin. Without technology, digital and physical drug trading would evolve, and without both cybercrimes and drug trading, money laundering methods would not have expanded and evolved throughout the years.

2. Cybercrimes

Cybercrimes are one of the biggest threats currently facing the world. Cybercrimes caused losses that amounted to $400 billion in 2005, compared to the $17 billion loss from the 9/11 attacks[4]. Internet-facilitated crimes are limitless; new crimes are committed every minute around the world from different locations. The cyber world offers opportunities to everyone: criminals can continue their criminal activities, traditional crimes can advance and become cybercrimes, and non-criminals can learn how to be criminals with the push of a button[3]. Nuth(2008) also argues that the cyber world enables
criminal offenses and makes them increasingly possible, creates new crimes, and transforms traditional crimes into advanced crimes.

Furthermore, McQuade(2001) writes that cybercrimes are very complex and mysterious to government officials, media, and society due to the involvement of advanced and complicated technologies with which many people are unfamiliar; the involvement of many suspects and victims, and the vast amount of damage and harm caused by and to them; the mixed varieties of traditional and new crimes; the lack of communication between law enforcement experts; and the ability of cybercrimes to occur from different geographical locations and different jurisdictions where law enforcement agencies can practice their authority. McQuade(2001) also suggests that adaptation to new technologies can generate crime waves, which in theory can be predicted and measured. Although these waves benefit transnational crime groups, terrorist groups, and cyber criminals, police and law enforcement agencies can sometimes use them in their favor to predict, prevent, and minimize the damage of certain cybercrimes. According to Nouh, Nurse, Webb, and Goldsmith(2019), there is an asymmetrical relationship between cyber criminals and law enforcement agencies, as law enforcement agencies face restrictions that do not allow them to collect data to investigate.

Cybercrimes and cybercriminals experience more benefits than traditional crimes. According to Li(2018), the sophistication and skills that cybercrimes require to offer many advantages to cybercriminals. For example, cybercrimes do not require physical appearance and can operate remotely across multiple time zones and jurisdictions, which makes it difficult for law enforcement to deal with those types of crimes[4]. Moreover, cybercrimes provide cybercriminals more anonymity. Cybercriminals operate from different locations around the world, and they can change their IP addresses and conceal them with a press of a button, making them effectively immune to detection and tracing[4]. Although it takes seconds to commit a cybercrime, cybercrimes can cause damages that last for weeks or even months. Once a network is infected with viruses, these viruses keep regenerating and spreading, causing more damages over time[4].

Furthermore, cybercrimes provide concealed victimization, as victims are attacked with little or no information on who attacked them. This concealment leads many victims to not report the crimes committed against them, which increases the dark figure of crime[4]. Kang(2018) argues that some victims are not willing to report and become hidden victims due to the ignorance of cybercrimes among police, limited accessibility of police and courts, and fear. Li(2018) found that as a result, only 1 in 100 cases was detected in the US, 1 in 8 was prosecuted, and 1 in 33 prosecutions resulted in prison time, and the chance of cybercriminals being sent to prison is 1 in 26,400.

Cybercrimes can be understood according to multiple criminological theories. According to McQuade(2001), theories and criminological schools from the 18th century can be applied to understand cyber criminals. For example, the classical school can explain cybercrimes by simply demonstrating the free will and the thrill-seeking actions accompanied by selfishness and evilness. Meanwhile, Sutherland’s(1947) differential association theory explains how some cybercriminals learn the basics of technology and continue their way into criminality[2]. McQuade(2001) notes that even Cohen and Felson(1979) mentioned technology, exploring how motivated offenders can attack suitable targets using technology and committing cybercrimes to take advantage of the absence of protection.

Cybercrime has been defined in many different ways in the scholarly world. According to Nuth(2008), cybercrimes are any type of crime conducted on the Internet, which requires hardware or physical technology such as a computer. In their works, Brar and Gulshan(2018) both argue that cybercrimes are malicious activities that affect the three fundamental principles of network security: confidentiality, integrity, and availability. According to Brar and Gulshan(2018), confiden-
tiality is threatened by attacks on private documents and passwords, integrity is threatened by attacks that aim to corrupt and destroy data, and availability is threatened by attacks that can immobilize or jeopardize the flow of data or information. Additional scholars such as Thomas (2018) define cybercrime as any offense enabled by technology. Meanwhile, Cordova, Alvarez, Ferrandiz, and Perez-Bravo (2018) define cybercrimes using the Oxford Dictionary of Law (2002), which defines cybercrimes as “any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.” Cordova et al. (2018) also expand upon this definition by stating that cybercrimes are any criminal act conducted in cyberspace, and they define cyberspace as the network that includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries [5].

Technology has facilitated cybercrimes because it gave birth to them. Nuth (2008) emphasizes one of many types of cybercrimes known as viruses. According to John (2006), a virus is malicious software that inserts its code and infects the area, causing damages. Nuth (2008) provides the example of a virus called “love bug.” Love bug was sent as an attachment in the year 2000 via email. Many people received the email and clicked the attachment files that contained the virus, causing millions of computers around the world to be damaged and infected within hours. Many governments and companies were attacked by this virus, and the worldwide business community lost an estimated $6.7 billion in the first five days of the spread of the virus. Furthermore, Nouh et al. (2019) share that cybercrimes marked 50% of crimes committed in the United Kingdom in 2017 alone and that almost 68% of businesses located in the UK have been victims of cybercrimes and cyber-attacks.

Cybercriminals adapt and evolve along with the evolution of technology. According to Glenny (2008), cybercriminals used to commit cybercrimes to ruin someone’s day in order to entertain themselves and enjoy a good laugh. However, the evolution of technology created many opportunities for cybercriminals to expand the field of their criminal activities [3]. With the huge dependence on technology and computers for everyday activities such as banking, texting, and sending and receiving emails, and the overall central role technology now plays in life, cybercriminals evolved from criminals who once just wanted to ruin someone’s day, to criminals who want to benefit and act upon opportunities that the evolution of technology offers [3]. Cybercriminals are ultimately very fast to adapt. By the time a new technology emerges, cybercriminals will have already coded programs, made plans, and generated new ideas on how they can benefit from this opportunity [6]. Examples include cyber-attacks on governments to achieve political goals, cyber-attacks on banks and credit cards to achieve a financial goal, and cyber-attacks on individuals to blackmail or achieve a personal goal.

According to Brar and Kumar (2018), cybercrimes always attack three fundamental principles, known as the CIA (confidentiality, integrity, and availability). Confidentiality means that cybercriminals will attack data that are private and limited to authorized users only, including account passwords. Names for those attacks can be eavesdropping, snooping, or password attacks [7]. Integrity refers to the accuracy of the attack and its occurrence in a specific time to achieve a specific goal. An example is an attack that shuts down electricity in an area for a few hours, and names for such attacks include Salami attack, cross-site scripting, and session hijacking [7]. Finally, availability means shutting down the access of authorized users from the attacked network so cybercriminals can roam without interruptions. Examples include shutting down Internet connections in a specific bank to block the access for the cybersecurity team, which allows cybercriminals to roam freely. Such attacks are called DDoS attacks, UDP attacks, and HTTP attacks [7].

There are many types of cybercrimes committed by cybercriminals, and categories of cybercrimes differentiate in both goals and means. Previous research from Nuth (2008) and Brar and Kumar (2018) provide that many
types of cybercrimes can be categorized into four main categories: entertainment, personal, financial, and political. Entertainment cybercrimes are any crimes to corrupt or ruin someone’s property. This includes cyber-vandalism, which is any malicious destruction of property[3]. Personal attacks are any attacks that achieve personal goals for the criminals. These attacks can include many cybercrimes, such as cybertrespass, which means crossing unauthorized boundaries.

Further crimes that fall under the personal category are child pornography, cyber stalking, cyber bullying, spying, and revenge[3][7][8]. Financial-gain attacks include any cybercrime that achieves financial gain for the criminal. These attacks include credit card theft, identity theft, fraud, electronic money laundering, and spam emails[3][7]. Finally, political cybercrimes are politically motivated crimes that aim to harm, sabotage, or cause financial damage. Examples include hacking and spying[3][7]. There are some cybercrimes that can be categorized in more than one category. For example, hacktivism (any network attacks that give access of private data and information to cybercriminals) can be used in any category of the above to achieve various goals that cybercriminals aim to achieve.

Cybercrime incidents happen globally, and the world has witnessed many of them. The first cybercrime case explored in this paper is the case, covered by Stevens(2011), of Joe, an Australian man who was arrested and sentenced for involvement in child pornography. Joe’s computer was seized by the police, and they found images that included child pornography. Joe’s life changed after his arrest: he was forced to sell his house to meet legal fees, he was prohibited from meeting his 8-year-old daughter without supervision, and he was forced to quit his job for “security reasons.” The second case comes from the FBI: a $10 million hack in 1994 by a transnational gang. Led by a Russian computer programmer, gang members hacked bank accounts from the United States by obtaining IDs and passwords and transferred all funds overseas. Although many receiving bank accounts have been frozen by authorities, the heist continued for months, until Levin the programmer was sent back to the US and pled guilty. Bellisle(2017) also tells the story of a member of the Russian parliament who hacked more than 500 U.S. companies and stole millions of credit cards that he then sold to other websites. A further example comes from the Department of Justice(2018), which covered a notable case of cyberstalking. Joel Kurzynski was arrested and sentenced for cyberstalking by threatening, body shaming, and sending hate speech to two close people in his life. Also, in a case with the Department of Homeland Security(2012), a group of people hacked credit cards and increased their limit. While acquiring the PIN, the organized group burned the information into new cards and drained them at ATMs. This operation was happening in 24 countries, resulting in a $40 million loot from 34,000 ATMs. Finally, the news has recently covered many cyber-attacks targeting big brands and countries. For example, Adobe was attacked, and 150 million accounts were leaked[9]. Sony PlayStation network, Target, Yahoo, and Marriott were all also victims of cyber-attacks and had their customers’ information leaked or hacked[9]. South Korea and Russia, in particular, have been targeted for cybercriminals, as 100 million credit cards were stolen in South Korea and 1.2 billion logins from 420,000 websites were possessed by hackers in Russia[9].

3. Drug Trafficking

Drug trading and drug smuggling are the second types of transnational crime that has been heavily facilitated and improved with technology. According to Nuth(2008), technology enables traditional crimes to transform and adapt to technologies. Drug trading and smuggling, like other crimes, have evolved and adapted along with technology. A review of previous research and known cases reveals how both hardware technology and software technology have modernized the illegal drug industry.

The United Nations Office of Drugs and Crime(2010) defines drug trafficking as the
global industry of illegal drugs that includes any cultivating, manufacturing, distributing, and sale of substances that are prohibited by laws. Although this definition is applied to traditional drug trafficking, the definition can also be applied to advanced drug trafficking with the way technology has evolved the illegal drug industry, as the same processes of trading and smuggling are relevant.

Technology-facilitated drug trafficking and smuggling use both physical or hardware technology and digital or software technology. Hardware-facilitated drug trading and smuggling refer to how traffickers and smugglers use technological machines and devices to seal their deals. These devices can include flying drones that carry the shipment and transport drugs in and out of any areas that include borders, walls, buildings, and fences[10]. Digital or software drug trading can be implemented by organized crime groups or dealers via the use of Internet and darknet, which provides suppliers the ability to advertise and show their products along with ratings and prices[11]. Customers can browse, ask, bargain, buy, and even share opinions with other costumers. All these deals happen with the click of a mouse from a computer connected to the Internet, without the need of leaving the house of even desk chair[11].

There have been many cases of drug trading and smuggling around the world in which criminals utilized technology to commit their crimes. For example, a 25-year-old man in 2017 was charged with drug-smuggling crimes in San Diego, where he smuggled more than 13 pounds of methamphetamine believed to be worth $46,000 using a drone that flew across the border[12]. According to Fiegel(2017), in 2012 alone, the US authorities seized 150 drones carrying two metric tons of marijuana, cocaine, and heroin. The drones mainly fly from Mexico to the United Stated carrying a variety of illicit drugs. Mexico upgraded the drone designs and increased the capacity compared to regular personal drones. Mexican drones now can carry and transport 60-100 kilograms[132-220 lbs.] of drugs in a single trip[13]. Drones offer organized crime groups and cartels less risk in drug trafficking. Firstly, they offer protection to employees and the whole group, as captured employees will be questioned by authorities[13]. Fiegel(2017) also notes that beyond transporting drugs, drones can work as a tool for surveillance that supports protecting areas and shipment. He offers the example of cartels that used drones to gather intelligence and scan the area to protect their $30,000,000 cocaine shipment going to Panama.

In addition to drones and hardware technology, drugs can also be traded online via the Internet. Augusto and Godoy(2015) reveal that the virtual drug black market can be accessed with fake IP addresses. For example, Silk Road referred to as “the Amazon of illicit goods,” attracts customers and suppliers from around the world buying and selling illicit items such as body parts, organs, and drugs[14]. Weed, ecstasy, heroin, steroids, cocaine, and hash are all traded on the website with full anonymity for the administrators, consumers, and suppliers[14]. With the use of Bitcoin as the main currency of payment, all payment transactions are fully untraceable and anonymous[14].

Moreover, Rhumorbarbe, Staehli, Broséus, Rossy, and Esseiva(2016) claim that the darknet has more than 48,000 listings of people who claim that they sell drugs from 70 countries. The most commonly listed drugs are cannabis-related drugs, ecstasy, and cocaine. Buskirk, Naicker, Bruno, Burns, Breen, and Roxburgh(2016) argue that after monitoring 16 illicit marketplaces across the darknet, they found that cannabis, pharmaceuticals, MDMA, cocaine, and methamphetamine had the highest demand. Although many virtual illicit market places such as Silk Road and Silk Road 2.0 were shut down by authorities, illicit market places are still growing and generating[15]. Affilipoaie and Shortis(2015) outline the steps needed to purchase illegal drugs from the darknet. An individual should use TOR browser to hide his or her IP, acquire Bitcoin for a fully anonymous transaction, and communicate via PGP encryption(short for Pretty Good Privacy) to ensure privacy and security from third parties.
Technology-facilitated drug trafficking is directly connected to cybercrimes. Cybercrimes are any illegal act that occurs via or in cyberspace[5] and without cyberspace, drug suppliers and consumers would not be able to seal their deals and exchange payments. Technology gave rise to cybercrimes, and cybercrimes, in turn, gave rise to the darknet and illegal e-commerce websites, where technology-facilitated drug trafficking flourishes.

4. Money Laundering

Money laundering is the process of “washing” illegally obtained money to make it appear legal and legitimately obtained in order to avoid prosecution[16]. Money laundering is the third type of transnational crimes that have been heavily facilitated by technology, and its placement as third on the list mirrors the underground economy[11]. Every illegal act that has a financial goal will resort to money laundering in order to complete its mission. No matter the type of crime, money laundering will always play the last part in order to make the outcome legal. Both cybercrimes and traditional crimes utilize money laundering to complete their purposes.

Naim(2005) argues that new technologies have facilitated money laundering due to the lack of physical borders and low-priced bank transactions. He also argues that due to new technologies, many financial institutions can be a destination of funds. As technology renders borders useless, criminals engage many offshore firms to launder their money remotely[11]. Albanese(2011) also notes that entertainment technology such as casino chips are heavily used by criminals to launder their money because gambling chips can be traded with cash. Also, Albanese(2011) states that criminals take advantage of money orders and checks by transferring their hard cash into official financial documents. Further types of money laundering facilitated by technology occur via cryptocurrencies or digital currencies.

Examples and cases of technology-facilitated money laundering are numerous, and many criminals have been globally prosecuted due to their involvement in laundering funds. For example, many online video games are involved in money laundering. According to Osborne(2019), cybercriminals steal credit cards and buy items in videogames such as Fortnite to launder their money. She shares that criminals buy V-Bucks that can be sold to the gaming community with lower prices, which provides criminals the perfect method to wash stolen funds. According to Hall(2015), discounted game codes are another method that criminals use to launder money stolen from credit cards. Hall(2015) argues that on websites such as Kinguin and G2A, people sell games at almost 80% discounts; however, the codes are obtained illegally and it is another method of laundering, which can be applied to anything in the e-commerce world. Due to the privacy that cryptocurrencies provide, criminals have been able to launder $1.2 billion between 2017 and 2018[28]. Ngetich (2018) highlights that with the help of Bitcoin, a Danish bank called Danske was able to launder $234 billion between 2007 and 2015. Gola(2019) and Beedham(2019) found that 7,096 out of 417,465 money laundering cases in Japan involved Bitcoin.

Money laundering is directly connected to cybercrimes and drug trading. As previously mentioned, money laundering is the resort of almost every single crime driven by finances, particularly cybercriminals who are involved in scamming and identity theft for monetary gains. Meanwhile, online drug traders and traffickers also commit their crimes in cyberspace with the help of cybercriminals for money and subsequently launder money in order to achieve their financial goals. Therefore, the connection between cybercrimes, drug trading, and money laundering is fundamentally established with the help of technology. Beyond the facilitation of individual crimes, technology has connected the dots and established interdependency and symbiosis between the three types of transnational crimes.
5. Policy Implication

There have been many attempted policies to defend against the three types of transnational crimes, but most have not been effective. Regarding cybercrimes, Nouh et al. (2019) argue that cybercriminals adapt to new methods 200% faster than authorities. No matter how authorities try to defend against and investigate cybercrimes, they are restricted and limited to the data they can access, which results in an asymmetrical relationship against cybercriminals. Brar and Kumar (2018) also study how authorities focus on cybersecurity to defend data against cybercriminals. Due to the fast adaptation of criminals, cybersecurity will not be enough to counter cybercriminals, because cybercrimes are not single-angled. Furthermore, Thomas (2018) argues that even if authorities succeed in countering cybercriminals, authorities will not be able to arrest and prosecute offenders due to jurisdictional limitations, because cybercrimes are digital and not limited to physical borders.

Policies have also failed to counter technology-facilitated drug trafficking. In traditional drug trafficking, authorities always focus on the supplier. Although traditional drug trafficking requires physical appearance and physical effort, suppliers continue to multiply in numbers due to the high demand. By default, cyber drug trafficking provides less risk and less effort to suppliers due to the lack of physical interaction, appearance, and borders. Unfortunately, authorities continue to target suppliers and ignore the bigger picture, which is approaching the issue through supply, demand, regulations, and completion.

Albanese (2011) argues that increasing efforts against money launderers will increase the number of transactions money laundered do to wash money. With the increase of transactions, fees increase; and when fees increase, money launderers earn more money, and the washing process continues.

Recommended policy interventions against cybercrimes should focus more on awareness and education for law enforcement, potential offenders, and victims, and more on cooperation between law enforcement agencies, nations, and the private sector. Thomas (2016) argues that many law agencies’ personnel are not properly educated and aware of cybercrimes, which makes victims more vulnerable to blackmailing and harassment. Also, Ron, Fuertes, Bonilla, Toulkeridis, and Javier Díaz (2018) note that nations such as Ecuador treat cybercrimes under civil law, which punishes cybercriminals with minor penalties if prosecuted. Criminalizing cybercrimes will not be accomplished without increasing awareness and education of cybercrimes’ consequences. Li (2018) provides a critical point regarding defense against cybercrimes. He mentions that a few countries have updated their laws in order to criminalize the crimes that are facilitated by technology. Li (2018) also suggests that a collaboration between both the public and the private sectors should occur to protect against cybercrimes.

Furthermore, Nouh et al. (2019) state that sharing intelligence between local and international law enforcement agencies is key to minimize the effect of cybercrimes. As an example, the FBI hosted a campaign, the Cyber-citizen Partnership Awareness Campaign, to increase the education and awareness of children and their parents on how to use the Internet ethically and avoid criminality and victimization. Glenny (2008) also provides advice on how to avoid being a victim of cybercriminals. He warns youth not to download illegal music and pornography, because they are largely used as baits to lure young people and make them vulnerable to hacking. Kang (2018) also provides extensive advice on how people should protect themselves from cyber-attacks. After analyzing the Hollywood hacking campaign that targeted famous personalities, Kang (2018) warns not to get baited by “phishing” emails that tend to hack computers and access all data that users have in their computer or on their associated cloud storages. Recommended policy interventions against cybercrimes should be approached from the victims’ side and not the offender’s sides.

Regarding both physical and digital technology-facilitated drug trafficking, new policy interventions should focus more on the demand and regulations, and less on the supply.
Fiegel(2017) and Wolfe(2019) mention how drug cartels use the technology of drones to transport drugs and surveil the areas to execute their mission. The demand is high for drugs, and as Albanese(2011) argues, focusing only on suppliers while ignoring demand will increase the prices and make criminals make more money. Therefore, new approaches should focus on where those drones are going, as focusing on the demand will render the suppliers’ operations useless. Meanwhile, limited existing research has specifically focused on how to counter digital drug trafficking. According to Albanese(2011), focusing on the demand and increasing internet use regulations is a better approach than targeting suppliers, as suppliers can be making deals from any point on the globe in different jurisdictions, which prohibits authorities from operating effectively. However, they can target the destination of the shipment within their jurisdiction and control the demand.

Recommended policy interventions for technology-facilitated money laundering have been previously raised by Naim(2005), Glenny(2008), and Albanese(2011). They all highlight that most money laundering occurs overseas from offshore companies, which will not happen if countries increase the sharing of their financial information. Such an approach also applies to digital money laundering that uses games’ codes and cryptocurrencies. Increasing communication between nations and companies can, by default, increase the awareness of consumers on how criminals steal credit cards using cybercrimes and launder them in video games and cryptocurrencies. Also, technology can provide banks and authorities with anti-money laundering methods. According to Balooni(2017), technologies can provide financial institutions with large data memory that can store, render, profile, and detect huge numbers of electronic transactions occurring by the minute around the world. Technology is capable of undergoing tasks that humans cannot process, and tracking money laundering transactions in vast numbers is one of those tasks that technology can help us to overcome.

6. Conclusion

All cybercrimes, drugs trafficking, and money laundering are facilitated and connected by the evolution of technology. Technology gave birth to cybercrimes, cybercrimes are used as a portal for drug trafficking, and both crimes resort to money laundering to finish the job and loot their funds legally. Therefore, the recommended policies to counter the three types of crimes should include a focus on consumers, victims, potential offenders, and regulations to prevent the spark that ignites those crimes. Education, awareness, and international/private collaborations should be encouraged to share intelligence between jurisdictions and to warn the youth and the elderly in particular, who are not familiar enough with technology to understand how not to violate the law or be victimized. The best method to fight any type of transnational crimes is to approach and analyze the whole equation, which should involve supply, demand, regulations, and victims (if they are not victimless crimes).

7. References

7.1. Journal articles


7.2. Books

and Copycats are Hijacking the Global Economy. Doubleday (2005).

7.3. Additional references


Lead Author
Mohammed Alqahtani / Florida International University
B.A. University of Miami
M.A. American University

Research field

Major career
- 2019~present. Florida International University, Teaching Assistant

Co-Author
Raymond Doug Partin / Florida International University
B.A. The University of Cincinnati
M.S. The University of Cincinnati

Research field

Major career
- 2018~present. Florida International University, Teaching Assistant

Correspondence Author
Back Sin-chul / University of Scranton Assistant Professor
B.S. Northeastern University
M.S. Bridgewater State University
Ph.D. Florida International University

Research field
- Low Self-control, Social Learning, and Texting While Driving, American Journal of Criminal Justice, 44(2) (2019).

Major career
- 2011~2012. Massachusetts State House, Legislative Aide
- 2019~present. University of Scranton, Professor

Co-Author
Jo Sung-gu / Kyungwoon University Professor
B.A. Kyungwoon University
M.A. Kyungwoon University
Ph.D. Kyonggi University

Research field
- Korea’s National Security and Anti-terrorism Strategy - The Cases of Key Figure Assassination and the Direction of Protection Security Activities-, Korean Police Studies Review, 17(2) (2018).

Major career
- 2006~2009. Republic of Korea National Assembly, Secretary
- 2012~present. Kyungwoon University, Professor