CrimRxiv

Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context

R.V. Gundur[1], Michael Levi[2], Volkan Topalli[3], Marie Ouellet[3], Maria Stolyarova, Lennon Yao-Chung Chang[4], Diego Domínguez Mejía[1]

[1]Flinders University, [2]Cardiff University, [3]Georgia State University, [4]Monash University

Published on: Apr 16, 2021

DOI: 10.21428/cb6ab371.5f335e6f

View the Executive Summary

Acknowledgements

This work was supported by the UK Home Office through a National Cyber Security Programme research grant. Research assistance was provided by Tessa Cole and David Flint. Editorial assistance was provided by Isobel Scavetta.

Introduction

Policing Cybercrime

Although the rate of most crimes appears to have been decreasing over the past three decades, the same cannot be said for cybercrimes (Van Dijk, Tseloni, and Farrell 2012, 245). The increase of digital aspects in everyday life has made crime and victimization in cyberspace a regular occurrence (Bryant and Bryant 2016). To that end, the rate of cybercrime has been steadily increasing over the past decade, and continues to be likely underreported (Caneppele and Aebi 2017; Levi et al. 2017; Levi 2017). Prior to the COVID-19 outbreak, during which the number of incidents of cybercrime in the UK had increased (Buil-Gil, Miró-Llinares, Moneva, Kemp and Díaz-Castaño 2020), incidents had been falling in England and Wales, though cybercrime still represented a larger proportion of all reported crime. The number of victims of total crime Telephone-operated Crime Survey for England and Wales (TCSEW) including fraud and computer misuse decreased by 19% in April to June 2020 compared with January to March 2020 (ONS, 2020). This is also true for the small number of countries which conduct general social survey measures of cybercrime as part of their general crime surveys or as separate modules on sub-sets of cybercrime such as identity crime. (See also successive Eurobarometer surveys for data within the EU 28 as a whole.) An increase in cybercriminal activity means that transactions that involve the proceeds of crime increasingly occur in whole or in part in cyberspace (Ablon, Libicki, and Golay 2014; Allodi, Corradin, and Massacci 2016; Higbee 2018; Hill 2018).

The uptick in cybercrime has resulted in the formation of digital policing units and computer emergency response teams (CERTs) in jurisdictions around the world (Harkin, Whelan, and Chang 2018; Boes and Leukfeldt 2017; Décary-Hétu 2016), as well as within industry (Holt 2018). Despite the increase in such units and cybersecurity spending, global law enforcement and private capacity to investigate and police cybercrime competently are not sufficient to respond efficiently in real time

(McMurdie 2016), due to the quickly-evolving and vast nature of these crimes (Holt 2018), which typically involve more effort and cross-border expense and access difficulties than do most offline crimes in the Pursue mode. Policing has been slow to adjust to the rise of digital crimes and fraud, not least because it often means giving up functions currently performed, which meet resistance (HMICFRS 2019a, 2019b). “Effectiveness” in policing cybercrime needs to be clearly defined and should be seen on a spectrum. The evolution of cybercrime and cyber offender strategies is fast paced, making studying and reporting on them a difficult task. In addition to this challenge, the vast majority of research is undertaken, produced, and disseminated in English and focuses on a minority of sites where actively publishing western academics are based (Cross 2018).

Yet, the scope of cyber offenders, their involvement in a range of illegal activities, and the costs of policing cyber offenders, stemming from cross-jurisdictional offences, generate serious concerns for law enforcement agencies throughout the world (Carroll and Windle 2018; Gilmour 2014; Malby et al. 2013). However, little is known about the attitudes of law enforcement towards cyber offenders in those countries in which state-sponsored and state-tolerated cyber offending occurs: it is simply assumed or inferred from unsuccessful pursuit that little is being done there, at least until they victimise their local populations, setting aside often well-informed and severe reactions to those deemed to be “political opponents” or acting without authorisation from those in power. Cyber offenders operate broadly across borders, creating mutual legal assistance problems, which arise from variation in legal definitions provided by different statutes (Harkin, Whelan, and Chang 2018; McMurdie 2016) as well as institutional problems of conflicting priorities even where the offenders are *not* state-sponsored or state-tolerated/corruptors. Except where political pressure or comity can be applied from abroad, enforcement agencies generally prioritise their domestic cases over international ones. As a result, cyber offenders encounter police services that differ in their approaches for detecting, investigating, and disrupting incidents associated with cyber offenders and their collaborators/competitors. These discrepancies, in turn, lead to uncertainties about the use of disruption strategies and their effectiveness, particularly in cross-border contexts, in addition to any uncertainties for evaluations arising from uneven but generally poor data availability.

With limited resources and expertise, especially in opportunity principle countries where discretion is formally allowed,[1] law enforcement must make explicit or implicit strategic decisions in its approach, focusing on what it believes will yield the largest impacts while working within the political and economic constraints of its local jurisdictions. Law enforcement alone is ill-equipped to provide comprehensive protection against attacks in cyberspace (Boes and Leukfeldt 2017; Broadhurst 2006). Understanding this reality (and in some cases seeing an opportunity for marketing their security services, especially in the aftermath of high-profile breaches), private companies and security firms invest billions of dollars in cybersecurity programs designed to monitor cyberspace for breaches, search for and patch vulnerabilities, and develop assets to protect against and respond to the large array of potential cyber-dependent and cyber-enabled threats.

Yet, despite continuing calls for increased and improved police cooperation and public-private partnerships (PPPs) (EUROPOL 2018), such cooperation is handicapped by the complexities of unhomogenised criminal statutes, policies, and regulations, coupled with the time required to prepare for and actually engage in successful international cooperation (Boes and Leukfeldt 2017; Malby et al. 2013). Given the lack of public information available on cooperation, these partnerships are difficult to systematically identify and assess. The transnational character of many cybercrimes complicates how law enforcement organizations cooperate and respond to cybercrime offenders and victims (Levi et al. 2015; Cross and Blackshaw 2015; Chang 2012). In addition, a chronic issue that law enforcement faces in regards to cybercrime is attributing crimes to the criminal actors responsible (in fact and in terms of evidential rules), thus rendering their capture and prosecution difficult even if mutual legal assistance were financially feasible on a practical basis at scale (Europol 2015). It is unlikely significant advances in attribution can be easily and effectively made in the short term. Accordingly, near-term strategies to combat cybercrime must focus largely on prevention and disruption, and on resilience.

Despite ongoing challenges in terms of resources and cooperation, transnational cybercrime enforcement has produced significant accomplishments, with successful takedowns of notable cryptomarkets, including AlphaBay, Hansa, and RAMP, as well as the Avalanche cloud-based bulletproof hosting service (EUROPOL 2018). However, little is known about how cyber criminals, who depend on such platforms and who evade law enforcement operations, displace their activities following the seizure of these services. Anecdotal evidence points to displacement to services that are in Eastern European countries including Russia, Ukraine, and Moldova, where enforcement and/or regulation appear to be lax or non-existent (Leyden 2017).

Though it is important to guard against the assumption that all crime groups are flexible geographically, it is likely that, as law enforcement improves at the country and regional level, some cybercriminals, not bounded by physical boundaries and engaged in scams or activities that are not geographically dependent for their success, transplant the bases for their criminal activities and operations to countries with weaker enforcement, legislation, and security regimes (Boes and Leukfeldt 2017). Despite such likely displacement outcomes, research on cyber offenders and their victims typically focuses on select case studies in specific geographical areas. Consequently, researchers have allocated relatively few resources to studying non-Western cyber contexts and non-English speaking contexts (Kshetri 2013, 2015; Cross 2018; Smith, Cheung, and Yiu-Chung Lau 2015).

Current research identifies various types of cybercrimes (Trend Micro 2016; Wall 2007; Wilson 2008; Yar 2013; Brenner 2010; Sood, Bansal, and Enbody 2013), their scripts and business models (Soudijn and Zegers 2012; Leukfeldt, Lavorgna, and Kleemans 2017; Warren et al. 2017; Kshetri 2010; Chaudhry 2017; Hutchings and Holt 2015), how criminals become involved and interact among themselves (Goldsmith and Brewer 2015; Lusthaus 2018; Broadhurst et al. 2014), the relationships between criminal actors and their victims (Leukfeldt 2014; Whitty and Buchanan 2012), and, where relevant, the vulnerabilities these crimes exploit (Arora, Yadav, and Sharma 2018; De Groot 2019; Guitton 2013; Kharraz et al. 2015; Vasek, Thornton, and Moore 2014; Zimba, Wang, and Mulenga 2019; Chadd 2018; Jakobsson and Young 2005; Lathrop and Stanisz 2016; Ulsch 2014; Zimba and Chishimba 2019).

Financial Aspects of Cybercrime

This project is focused on the modest but emerging literature on the laundering of the proceeds of cybercrime (Bååth and Zellhorn 2016; Campbell-Verduyn 2018; Constantin 2017; Custers, Pool, and Cornelisse 2018; Fanusie and Robinson 2018; Hyman 2015; McGuire 2018, 2019). Among countries, there are variations in the legal definition of *laundering*, but most jurisdictions include self-laundering and any action to conceal or even simply move the proceeds of crime.[2] Evidently, cybercriminals implement a diverse array of economic transfer schemes. The strategies used are likely linked to the type of currency or digital asset received during the commission of a crime. To that end, it is imperative to investigate how cybercriminals use both crypto- and fiat currencies to accept and extort payment, transfer funds, and pay out on their obligations both to themselves and to others in their criminal supply chain.

Works Cited

Ablon, Lillian, Martin C Libicki, and Andrea A Golay. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: Rand Corporation.

Allodi, Luca, Marco Corradin, and Fabio Massacci. 2016. "Then and Now: On the Maturity of the Cybercrime Markets the Lesson That Black-Hat Marketeers Learned." *IEEE Transactions on Emerging Topics in Computing* 4 (1): 35-46.

Arora, Arushi, Sumit Kumar Yadav, and Kavita Sharma. 2018. "Denial-of-Service (Dos) Attack and Botnet: Network Analysis, Research Tactics, and Mitigation." In *Handbook of Research on Network Forensics and Analysis Techniques*, 117-141. IGI Global.

Bååth, David, and Felix Zellhorn. 2016. How to Combat Money Laundering in Bitcoin? An Institutional and Game Theoretic Approach to Anti-Money Laundering Prevention Measures Aimed at Bitcoin.

Boes, S, and ER Leukfeldt. 2017. "Fighting Cybercrime: A Joint Effort." In *Cyber-Physical Security*, edited by Robert M. Clark and Simon Hakim, 185-203. Switzerland: Springer.

Brenner, Susan W. 2010. "Three Categories of Cybercrime." In *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara, California: Praeger.

Broadhurst, Roderic. 2006. "Developments in the Global Law Enforcement of Cyber-Crime." *Policing: An International Journal of Police Strategies & Management* 29 (3): 408-433.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime." *International Journal of Cyber Criminology*: 1-20.

Bryant, Robin, and Sarah Bryant, eds. 2016. *Policing Digital Crime*. Surrey: Ashgate.

Buil-Gil, David, Fernando Miró-Llinares, Asier Moneva, Steven Kemp, and Nacho Díaz-Castaño. 2020. "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK." European Societies: 1-13.

Campbell-Verduyn, Malcolm. 2018. "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance." *Crime Law Social Change*: 1-23.

Caneppele, Stefano, and Marcelo F Aebi. 2017. "Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes." *Policing: A Journal of Policy and Practice*.

Carroll, Paul, and James Windle. 2018. "Cyber as an Enabler of Terrorism Financing, Now and in the Future." *Journal of Policing, Intelligence and Counter Terrorism* 13 (3): 285-300.

Chadd, Anthony. 2018. "DDOS Attacks: Past, Present and Future." *Network Security* 2018 (7): 13-15. https://doi.org/10.1016/s1353-4858(18)30069-2.

Chang, Yao-Chung Lennon. 2012. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar Publishing.

Chaudhry, Peggy E. 2017. "The Looming Shadow of Illicit Trade on the Internet." *Business Horizons* 60 (1): 77-89.

Constantin, Mircea. 2017. "Methods of Laundering Money Resulted from Cyber-Crime." *Economic Computation & Economic Cybernetics Studies and Research* 51 (3): 299-314.

Cross, Cassandra. 2018. "Marginalized Voices: The Absence of Nigerian Scholars in Global Examinations of Online Fraud." In *The Palgrave Handbook of Criminology and the Global South*, 261-280. Springer.

Cross, Cassandra, and Dom Blackshaw. 2015. "Improving the Police Response to Online Fraud." *Policing: A Journal of Policy and Practice* 9 (2): 119-128.

Custers, Bart HM, Ronald LD Pool, and Remon Cornelisse. 2018. "Banking Malware and the Laundering of Its Profits." *European Journal of Criminology*: 1477370818788007.

De Groot, Juliana. 2019. "A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time." *Digital Guardian*.

Décary-Hétu, David. 2016. Policing Cybercrime and Cyberterror. Taylor & Francis.

Europol. 2015. *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European Union Agency for Law Enforcement Cooperation.

---. 2018. *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European Union Agency for Law Enforcement Cooperation.

Fanusie, Yaya, and Tom Robinson. 2018. "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services."

Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop?. *Crime science, 7*(1), 1-4.

Gilmour, Stan. 2014. "Policing Crime and Terrorism in Cyberspace: An Overview." *The European Review if Organized Crime*: 143-159.

Goldsmith, Andrew, and Russell Brewer. 2015. "Digital Drift and the Criminal Interaction Order." *Theoretical Criminology* 19 (1): 112-130.

Guitton, Clement. 2013. "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?" *European Security*. https://doi.org/10.1080/09662839.2012.749864.

Harkin, Diarmaid, Chad Whelan, and Lennon Chang. 2018. "The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis." *Police Practice and Research* 19 (6): 519-536.

Higbee, Aaron. 2018. "The Role of Crypto-Currency in Cybercrime." *Computer Fraud & Security* 2018 (7): 13-15.

Hill, Julie Andersen. 2018. "Swift Bank Heists and Article 4a." *Journal of Consumer and Commercial Law* 22 (1).

Holt, Thomas J. 2018. "Regulating Cybercrime through Law Enforcement and Industry Mechanisms." *The Annals of the American Academy of Political and Social Science* 679 (1): 140-157.

Hutchings, Alice, and Thomas J. Holt. 2015. "A Crime Script Analysis of the Online Stolen Data Market." *British Journal of Criminology* 55 (3): 596-614. https://doi.org/10.1093/bjc/azu106.

Hyman, Mitchell 2015. "Bitcoin ATM: A Criminal's Laundromat for Cleaning Money." *St. Thomas Law Review* 27: 296.

Jakobsson, Markus, and Adam L Young. 2005. "Distributed Phishing Attacks." *IACR Cryptology ePrint Archive* 2005: 91.

Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. "Cutting the Gordian Knot: A Look under the Hood of Ransomware Attacks." International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

Kshetri, Nir. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. New York: Springer Science & Business Media.

---. 2013. "Cybercrime and Cybersecurity in the Global South: Status, Drivers and Trends." In *Cybercrime and Cybersecurity in the Global South*, 1-29. Basingstoke: Springer.

---. 2015. "Cybercrime and Cybersecurity Issues in the BRICS Economies." *Journal of Global Information Technology Management* 18 (4): 245-249.

Lathrop, Alex J., and Janine M. Stanisz. 2016. "Hackers Are after More Than Just Data: Will Your Company's Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations?" *Environmental Claims Journal* 28 (4): 286-303. https://doi.org/10.1080/10406026.2016.1197653.

Leukfeldt, Rutger. 2014. "Cybercrime and Social Ties." *Trends in Organized Crime* 17 (4): 231-249.

Leukfeldt, Rutger, Anita Lavorgna, and Edward R Kleemans. 2017. "Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime." *European journal on criminal policy and research* 23 (3): 287-300.

Levi, Michael. 2017. "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues." *Crime, Law and Social Change* 67 (1): 3-20.

Levi, Michael, Alan Doig, Rajeev Gundur, David Wall, and Matthew Williams. 2015. *The Implications of Economic Cybercrime for Policing*. London: City of London Corporation.

---. 2017. "Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research." *Crime, Law and Social Change* 67 (1): 77-96.

Leyden, John. 2017. "Bulletproof Hosts Stay Online by Operating out of Disputed Backwaters." *The Register*, 2017. https://www.theregister.co.uk/2017/10/05/bulletproof_hosting/.

Lusthaus, Jonathan. 2018. *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press.

Malby, S, R Mace, A Holterhof, C Brown, S Kascherus, and E Ignatuschtschenko. 2013. "Chapter Seven: International Cooperation." In *Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime*. Vienna: United Nations Office on Drugs and Crime.

McGuire, Michael. 2018. *Into the Web of Profit.* Bromium.

---. 2019. *Into the Web of Profit: Social Media Platforms and the Cybercrime Economy.* Bromium.

McMurdie, Charlie. 2016. "The Cybercrime Landscape and Our Policing Response." *Journal of Cyber Policy* 1 (1): 85-93.

ONS. 2020. *Crime in England and Wales: year ending June 2020.* Office for National Statistics.

Smith, Russell G, Ray Cheung, and Laurie Yiu-Chung Lau, eds. 2015. *Cybercrime Risks and Responses—Eastern and Western Perspectives*. New York: Palgrave Macmillan.

Sood, Aditya K, Rohit Bansal, and Richard J Enbody. 2013. "Cybercrime: Dissecting the State of Underground Enterprise." *IEEE internet computing* (1): 60-68.

Soudijn, Melvin RJ, and Birgit CHT Zegers. 2012. "Cybercrime and Virtual Offender Convergence Settings." *Trends in Organized Crime* 15 (2-3): 111-129.

Trend Micro. 2016. "The Many Faces of Cybercrime." https://web.archive.org/save/https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-many-faces-of-cybercrime.

Ulsch, MacDonnell. 2014. *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks*. Hoboken, New Jersey: Wiley.

Van Dijk, Jan, Andromachi Tseloni, and Graham Farrell. 2012. *The International Crime Drop*. New York: Palgrave Macmillan.

Vasek, Marie, Micah Thornton, and Tyler Moore. 2014. "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem." International conference on financial cryptography and data security.

Wall, David S. 2007. "Cybercrime Furthers: The Automation of Offender-Victim Engagement." In *Cybercrime: The Transformation of Crime in the Information Age*. Bristol: Polity.

Warren, Steve, Gavin Oxburgh, Pam Briggs, and David Wall. 2017. "How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?" International Conference on Human Aspects of Information Security, Privacy, and Trust.

Whitty, Monica T, and Tom Buchanan. 2012. "The Online Romance Scam: A Serious Cybercrime." *CyberPsychology, Behavior, and Social Networking* 15 (3): 181-183.

Wilson, Clay. 2008. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress."

Yar, Majid. 2013. *Cybercrime and Society*. Sage.

Zimba, Aaron, and Mumbi Chishimba. 2019. "On the Economic Impact of Crypto-Ransomware Attacks: The State of the Art on Enterprise Systems." *European Journal for Security Research*: 1-29.

Zimba, Aaron, Zhaoshun Wang, and Mwenge Mulenga. 2019. "Cryptojacking Injection: A Paradigm Shift to Cryptocurrency-Based Web-Centric Internet Attacks." *Journal of Organizational Computing Electronic Commerce* 29 (1): 40-59.

Project Overview

This project is an assessment of the current knowledgebase represented in the academic and grey literature regarding the financial aspects of various cybercriminal business models. It has three prominent characteristics: it is multilingual; it provides background on education, law enforcement strategy, and regulation vis-à-vis cybercrime in countries with significant internet user bases, and; it analyses how cybercriminals conduct financial transactions, to the extent of our understanding of these transactions.

Most research on cybercrime published within the academic and grey literature is in English. Accordingly, we have undertaken a systematic search to identify documents that address financial transactions in cybercrime. We have engaged in similar searchers in four additional languages: Chinese, French, Russian, and Spanish, to determine if there were concerns in these spaces that the English-language literature failed to consider. This research has made it clear that there is an ongoing need for more country- and region-specific research and for more multi-lingual analyses of cybercrime and related processes. Cybercrime can, and often does, transcends borders. While there exist reports within the grey literature that examine cybercrime and cyberthreats through a global lens, these publications often do not provide detail regarding significant local and regional considerations and may overlook concerns that may only have *prima facie* domestic or regional impacts.

Education, law enforcement, and regulation of countries that use the languages considered for administrative purposes and have more than 20 million internet users vis-à-vis cybercrime vary greatly. Developed economies are increasingly investing in cybersecurity and cybercrime prevention. In some cases, these governments rely on public-private partnerships to augment capacity. The production of government research varies considerably in terms of depth, frequency, and quality, but developed countries appear to be increasing law enforcement capacity to cope with cybercrime. However, our review also indicates that, despite calls for cooperation and capacity building, emerging economies continue to struggle to develop research and investigative units capable of doing the analysis that is undertaken in established economies. Awareness and in-depth analysis of these issues are low in English publications, which tend to focus disproportionally on English-centric data and concerns that affect the Global North.

While this project is limited by not including additional, commonly-spoken languages (e.g. Arabic and Portuguese), it shows that there is a significant weakness in cybercrime research in non-English contexts that must be considered as we think about cybercrime ecosystems. Should it persist, this failure will have an increasingly negative impact globally, particularly as more non-English speaking individuals from emerging economies join the ranks of everyday internet users. Their presence as potential offenders or victims in cybercrime is an issue that has received almost no attention to date.

Within the limitations within the literature we offer an analytical overview of the what is known, the lessons learned from the literature surveyed, and the outstanding gaps regarding transactions in cybercriminal activity. Driving our analysis are two questions. First, “How do cyber offender business models operate?” In considering this question throughout the research, we catalogue what is known regarding (a) how cybercriminals structure their financial operations (i.e., how money is obtained, transferred, and cashed-out; and the strategies, products, players, and services involved); (b) the role of virtual currencies and other technologies in existing offender models; and (c) how cybercriminal activity enables or interacts with offline or largely offline economic crimes, such as money laundering, fraud, extortion, and corruption. Second, “What are current law enforcement and industry practices aimed at disrupting these business models?” To evaluate these two questions throughout this project we catalogue what is known regarding (a) what evidence there is to determine how effective disruption approaches are in preventing offenders from obtaining, transferring, and cashing-out ill-gotten funds; (b) what we know about the extent of income or profits that offenders make from cybercrime; (c) how costs to offenders can be increased to reduce the rewards for committing crime; and (d) how political considerations, including political will and legislation, affect enforcement responses, including strategies employed, funding, and international cooperation.

Our analysis is tempered by the limitations of the extant literature. Many accounts of the financial aspects of cybercrime and what they entail – in all languages – are incomplete. Cybercrime research tends to focus on the commissioning stages of the offense up to the point at which victimisation occurs, but not beyond. Even when accounts are detailed, data sources are not transparent, and estimates often make assumptions regarding the prevalence, costs of operation, and costs of victimisation, all of which are inconsistently reported across the literature. Accordingly, our reviews and analyses of the research surveyed present what we know regarding how cybercriminals conduct transactions in their business models. As well, it identifies what still needs to be investigated to provide a better indication of what should be done to prevent harm and pursue successful criminals in the future.

The project proceeds with five sections that cover each language. Each language section provides:

1. an overview of the high-internet-user (>20 million) countries whose governments use the studied language administratively;
2. an accounting of the research strategy and results; and
3. an analysis of issues discovered in the literature that have to do with transactions in or affected by cybercriminal ecosystems.

Section I presents the English-language overview. This overview serves as a touchstone for our investigation. It focuses on seven countries: Australia, Canada, India, Nigeria, South Africa, the United Kingdom, and the United States of America. It presents a synthesis of the academic and grey literature available in English as it pertains primarily, though not exclusively, to the English-speaking world. It provides an overview of financial ecosystems and the properties of various types of currencies, a set of common cybercrime scripts, and a typology of transactions seen in the preparation and commission of cybercrimes. It also discusses the regulatory considerations that have emerged as a result of cybercrime.

Section II presents the Russian-language overview, which focuses on the English and Russophone literature that pertains to the topic of financial transactions in cybercriminal contexts in Russia. It shows that while there is good coverage of Russian issues in the English literature, some concerns expressed in the Russian literature or that impact upon specifically Russia are un- and underreported.

Section III presents the Chinese-language overview, focusing on Taiwan and mainland China. It provides an overview of the bodies that respond to cybercrime in both countries and the appropriate legislation. In addition, it surveys the available literature on transactions vis-à-vis cybercrime and IT related crime. It shows that the Chinese-language literature is still limited and that much of what we know vis-à-vis cybercrime in Chinese-speaking contexts is reported in the press. There are concerns regarding censorship and its impact in researching and publishing research on cybercrime.

Section IV presents the Spanish-language overview, focusing on Mexico, Colombia, Argentina, and Spain. It shows that the largest Spanish-speaking countries have all developed cybercrime policies designed to improve response capacity and regulation. Almost all behaviours observed in the English literature are also present in Spanish-speaking contexts, indicating that there is no language barrier in terms of accessing materials used to conduct cybercrime or methods of executing various cybercrimes.

Section V presents the French-language overview, focusing on Canada and France. There is little literature written in French vis-à-vis cybercrime; accordingly, the report offers a review of the existing literature and suggestions for how future research might proceed in this space.

This report concludes with a discussion that brings our findings together, showing how research in languages other than English complement and augment the English-language research, where gaps persist, and strategies to better conduct relevant research on the financial dynamics of cybercrime henceforth.

Section I: Lessons from the Anglophone Literature

Introduction

Most academic and grey literature on cybercrime is produced in English. This report surveys the existing English-language literature that contributes to our understanding of financial processes in, and leveraged by, cybercriminal activities. In completing this task, this report first discusses the methods and databases used to undertake this review and the limitations encountered in assessing some of the high-internet-user, English-speaking countries. Second, it provides an overview of the state of law enforcement and public information vis-à-vis cybercrime and financial crime related to cybercrime in the countries of focus. Third, it describes financial ecosystems and their relationships with cyberspace. Fourth, it presents what is known regarding the ecosystems of the crimes considered in this project. Fifth, it outlines the monies to be examined and their properties. Sixth, it presents the key issues that arose in the literature review, including a typology of transactions; claimed methods, tools, and services that facilitate the cashing out and laundering proceeds of cybercrime; and legal and financial regulations regarding these economic activities. Finally, it considers the questions proposed and discusses the limitations of the current English-language literature.

Methods

This report focuses on English-language sources that are produced around the world. It is presented together with multilingual research undertaken by the team in French, Russian, Chinese, and Spanish over the same topics. Specifically, this report surveys academic and grey literature that examines English-speaking countries with more than 20 million internet users in 2016 (approximations by the International Telecommunications Union (2019)): Australia (21M), Canada (33M), India (390M), Nigeria (48M), the United Kingdom (62M), and the United States (250M).

To identify recent (2014 through December 2019), relevant peer-reviewed, academic literature, the team devised an array of search terms relevant to the project at hand and engaged in a purposive sampling strategy. The search terms focused on crime types with clear financial elements. Terms included *inter alia*, ransomware, DDoS attacks, extortion, sales of drugs, weapons and other contraband in illicit marketplaces, fraud, online money laundering, fintech, and various crimeware-as-a-service types. Initially, the research focused on these issues within the geographical context of the United Kingdom. The terms were searched in eleven academic databases, using Boolean search combinations where permitted. The yield was small, with only 24 papers retained as being suitable for our research objectives from an initial screening. The search terms were refined three times in an effort to capture all relevant materials, but the yield did not greatly expand beyond what was initially identified.

The search was then expanded to include all English-language academic materials and the proceedings from relevant technological conferences (e.g. Institute of Electrical and Electronics Engineers (IEEE)) and supplemented with searches on specific terms and processes that were uncovered in the coding process. In addition to the scholarly research drawn from academic databases, the team also located whitepapers produced by both governmental and non-governmental organizations over the past 10 years, drawn from clearweb search engines, websites of the bodies that produced the resources, and the EC3 database on cybercrime, to which the research team had access; governmental policy briefs and legislation; and news generated by reputable news providers. The team also reviewed relevant English-language content produced by international bodies, including Europol and FATF-type bodies.

Overview of the literature

The English-language review focuses primarily, though not exclusively, on anglophone contexts; relevant content that focuses on other reports within this project – notably China and Russia – has been presented with those reports. The searches resulted in 335 English-language articles that were retained. Two analytical foci emerged after coding the retained documents: one examined the processes and attributes of the cybercriminal acts and what is known about the actors behind these acts, and the other examined the financial means which crimes that sought to generate profit used. In both cases, however, authors prioritised the front-end of the crimes, describing how attacks happen, vulnerabilities, and processes in broad terms. There appears to be little research that collects data that would facilitate the description and assessment of cybercrime scripts (Edwards 2016). To that end, there is limited specific information regarding the transactions and transactional methods that cybercriminals engage in after they obtain money as a result of their criminal actions. It is arguable that the academic focus reflects the mainstream policing focus, which is on predicate offenders and their prosecution rather than on the money trail. It also reflects the greater difficulties for observers in obtaining evidence on the money trail.

Accordingly, while authors identified scams, threats and crimes in cyberspace, emerging threats, and law enforcement investigation strategies or capacities, they seldomly provided specific, verifiable primary data. Notably, the grey literature did not provide transparent methodological approaches or data sources. Moreover, when reports provided estimates in terms of prevalence of cybercriminal tools and value loss, these numbers – with a lack of data – appeared to be, at best, educated guesses or, at worst, amplified numbers based on unlikely worst-case scenarios that overstated the plausible dynamics of the market (e.g. by assuming all advertised crimeware-as-a-service would be operationalizable or would operate as claimed). The production of reports by the private sector, governments, and think tanks tends to focus on emerging trends, often provides big-picture analysis, and is haphazard, with many reports or assessments providing one-off snapshots instead of being produced at regular intervals.

The nature of literature is such that Europol’s *Internet Organised Crime Threat Assessment* (IOCTA), produced annually since 2014, is the only ongoing, publicly-available threat assessment; there are no ongoing, in-depth examinations that document the rapid changes that occur within the cybercriminal ecosystem with a degree of detail that would allow independent researchers to confirm or refute the findings, nor are there comprehensive examinations of the cybercriminal financial strategies. Moreover, there is a certain degree of repetition in both the academic and grey literature, generally. Authors seem compelled to describe actions or artefacts that might have gained attention and were assumed to be unknown to readers; prominent examples from the research surveyed for this report include constant descriptions of how cryptocurrency and the blockchain work and defining new behaviours or criminal strategies.

In addition, research is geographically limited both in terms of where it is produced and the scope it has. Some governments provided occasional reports to assess issues related to cybercrime, but most did not; some of these reports are unavailable for public consultation. Except for analysis of regulatory frameworks which necessarily focuses on jurisdiction, most cybercrime research does not appear to focus on the geography of crime, except to provide broad claims of where certain actors might be located; this omission may be the result of the borderless nature of cybercrime. There are few notable exceptions where research attempts to explore cybercriminal behaviour ‘in’ Russia, China, and Nigeria, but even in those cases, analysis is limited, inconsistent, and sometimes superficial.

Moreover, while some reports note that there are an increasing number of victims in emerging economies, there is little exploration of the nature of the crimes or victimisation that impact these economies the most. Emerging economies’ populations are an increasingly large proportion of internet users. Accordingly, exploring how cybercrime affects these users and how it may emerge in these contexts is critical to understanding future cybercrime trends, including likely domestic political and law enforcement reactions in emerging economies which may clamp down on cybercriminals as a result (unless cybercriminals are state-sponsored or corruptly protected). Such attention is particularly important due to increased interconnectivity between developed and emerging economies, such as through diasporas and foreign direct investment. Crimes that target internet users within emerging economies are likely not only to appeal to cybercriminals but also to have international impact. Yet, many emerging economies lack the local knowledge to develop robust domestic or regional research programmes on cybercrime or cybersecurity. Failing to fill those needs, foreign researchers do not investigate cybercrime in these places in depth, nor do they engage in robust capacity building efforts in these countries.

The State of Play in Countries of Focus

This section provides an overview of relevant law enforcement bodies, access to public information, and socio-political considerations that may impact law enforcement activities and the generation of relevant public information in countries that produce government information in English and have internet user bases of more than 20 million people: Australia, Canada, India, Nigeria, the United Kingdom, and the United States.

In order to identify potential sources of government generated public information, the research team created an accounting of relevant government bodies in the countries of interest. Generally speaking, each country has at least three core bodies relevant to the themes of cybercrime and illicit or unregulated financial transactions relevant to this report: a general intelligence agency, a cybercrime law enforcement unit, and a financial crimes investigation unit. In some countries, such as the UK, there are a plurality of bodies that have cybercrime, cyber intelligence, and financial crime in their remit, sometimes specializing in specific crimes, such as fraud or tax crimes. Most information relates to cybersecurity strategies, which include how to create better “protect” and “prevent” models, and the front-end of cybercrimes where clear victims can be defined and where the points of contact between cyber offenders and their victims are studied. In general, the publicly available study of intermediary transactions, that involve the transfer of funds after a victim surrenders them, is underdeveloped, as is research related to intermediary parties that facilitate such transactions.

Among developing countries, the extent to which there is inter-agency cooperation within a country or among international counterparts is often unclear. Developing countries often lack public strategy documents, publicly facing information for the public, or publicly available reports on crime. Accordingly, it appears that public information production is often associated with developed countries that have bodies that demand information for accountability purposes from the government and/or law enforcement, and that have a more visible production of academic publications. Historically, there has been difficulty in developing effective mechanisms for Global South to Global North knowledge flows (Lor and Britz 2005), with researchers from, and research produced, in the Global South often being excluded from knowledge production unintentionally or otherwise (Lo 2011; Cross 2018). This limitation creates difficulties in identifying the nature and extent of cybercrime – both in terms of cybercrime generated and cybercrime experienced – in large internet-using populations in emerging markets, which appear, as is the case globally, to be growing, albeit at potentially a faster percentage rate from a lower base rate (Kshetri 2010, 2015). Moreover, the failure to include this research results in the overlooking of political and cultural considerations that may affect how offenders and victims behave and how authorities, with very different resources and obstacles respond to some cyber-related crimes. Such obstacles may include corruption (Goodman 2011; Lusthaus and Varese 2017), resource limitations (Speer 2000; Kshetri 2017), barriers to relevant and quality education (Catota, Morgan, and Sicker 2019; Irons and Ophoff 2016), a failure to support gender-related (i.e. women and the LGBTQI community) crime (Segrave and Vitis 2017), deficits in the rule of law (Goodman 2011), and kleptocracy (Cooley, Heathershaw, and Sharman 2018).

In this overview, we have focused on the government resources available in each country. We have drawn attention to memberships and agreements that countries have entered in the international sphere. Where relevant, we have drawn attention to domestic and/or regional political issues that impact capacity development. It is important to note that public-private partnerships are also commonly used to improve capacity. This report notes government use of such partnerships; however, documenting the breadth and characteristics of these partnerships – and their effects – is not possible. Finally, given the attention to cryptocurrency in the literature, we have also reviewed the regulations that pertain to cryptocurrencies for each country surveyed.

Australia

Cybercrime

Australia appears to be building and maintaining a strong cybersecurity system domestically and regionally, in its sphere of influence, and has been internationally cooperative. Australia has established relevant units throughout its law enforcement mechanisms, acceded to the Council of Europe's Convention on Cybercrime, known commonly as the Budapest Convention (Maurushat 2010), and signed the *Paris Call for Trust and Security in Cyberspace*, an initiative launched by French President Emmanuel Macron at the UNESCO Internet Governance Forum (IGF) that seeks to "establish international norms for the internet, including good digital hygiene and the coordinated disclosure of technical vulnerabilities" (Matsakis 2018). Moreover, Australia's enforcement bodies have participated in multinational investigations (Broadhurst 2017). It appears that Australia is monitoring a wide array of cybercrimes and is developing mechanisms to support domestic victims and to pursue foreign offenders, where plausible. The Australian government appears to engage with emerging and ongoing cybercrime-related issues by providing operational support and drafting legislation that facilitates prosecutorial abilities (Hooper, Martini, and Choo 2013; AUSTRAC 2018c).

Within its sphere of influence, Australia is positioning itself to be a leader in cybercrime enforcement and cybersecurity not only in terms of developing capacity within its own border but also within the Indo-Pacific region and internationally, e.g. via UNODC. The Australian government recognises that, although the country has a small population, its population makes a good target for cybercriminals since it is relatively wealthy. Moreover, the government appears to be fostering the domestic cybersecurity industry and is developing it in order to help respond to domestic, regional, and international cybercrime issues. The government, when reporting on crime, focuses on points of contact between the offenders and victims. Information, regarding the Australian Government's overarching strategies and outlooks, is easily available, though it is located in several locations, given that several government bodies work on and provide services related to cybersecurity and cybercrime.

These law enforcement, public service, intelligence, and investigative bodies include:

- **ACORN, the Australian Cybercrime Online Reporting Network**. ACORN is a national online system that allows members of the public to report instances of cybercrime. It also has public-facing information written for the public regarding specific types of cybercrime and how to protect against them. ACORN has provided quarterly statistics on major cybercrimes in Australia and has consistently identified scams, fraud, and bogus purchases/sales as accounting for 70% to 75% of reported cybercrimes since it began producing those quarterly statistics in March of 2015 (https://www.acorn.gov.au/resources).

- **ACSC, the Australian Cyber Security Centre.** The ACSC is a part of the **Australian Signals Directorate (ASD),** Australia's authority for cyber and information security. The ACSC is staffed jointly by ASD and **DIO, the Defence Intelligence Organisation.** The ACSC also carries out Australia's **CERT** services. The ACSC serves as an operational hub that is designed to facilitate the interaction between government and industry partners and to "facilitate faster and more effective responses to significant cyber incidents" (Australian Cyber Security Centre 2017).

> The ACSC is responsible for the website https://cyber.gov.au, which offers information for various public actors interested in obtaining information regarding cyber threats, advice on cybersecurity, and access to programs related to cybersecurity and ICT products. The ACSC also produces up-to-date reports on best practices, guidance, threats, and significant investigations that the body has undertaken.

- **ACIC, the Australian Criminal Intelligence Commission.** The ACIC (formerly known as the Australian Crime Commission) is Australia's national criminal intelligence agency. It estimates the cost of cybercrime to the Australian economy as $1 billion Australian dollars annually in direct costs alone and states that the principal threats from cybercrime are from overseas actors (Australian Crime Commission 2018).
- **AFP, the Australian Federal Police.** The AFP is the primary policing agency for policing serious and organised crime in Australia. It has Cybercrime Investigation teams that focus on cybercrimes that have "national significance." It participates in the Virtual Global Taskforce, an alliance of international law enforcement agencies and private sector partners, that combat child sexual exploitation. State police forces also include specialist units, such as Taskforce Argos of the Queensland Police, that investigate child exploitation material. Taskforce Argos of the Queensland Police was responsible for the takedown of the darkweb child exploitation website, Childs Play (Bleakley 2018). Neither the AFP nor Taskforce Argos produces publicly available reports.
- **ASIO, the Australian Security Intelligence Organisation.** ASIO has a cyber program that focuses on malicious state-sponsored cyber activity and cyber espionage, activities it views as increasing threats to Australia (2018, 2020).

- **DFAT, the Department of Foreign Affairs and Trade.** DFAT has a Cyber Policy Section, which is responsible for building capacity with international partners. It produced *Australia's International Cyber Engagement Strategy* (2017), a document that outlines how Australia views its role in cybersecurity in the international context. It states that the Australian government is working together with regional partners to improve connectivity and resource availability, particularly in countries where infrastructure is lacking. Another key issue involves helping countries in the region develop appropriate legislation and investigation to counter cybercriminal activity. Moreover, Australia is also developing better cybercrime prevention and detection strategies with its regional partners and actively supporting public-private partnerships to help improve awareness and responses (Department of Foreign Affairs and Trade 2017).

In addition to the law enforcement bodies that focus on cybercrime, there is also the **Australian Institute of Criminology** (AIC), an agency of the Australian Government, which commissions and produces a wide array of crime-related reports, including topics concerning cybercrime. The local academic production is robust, with world-recognised scholars producing both social-science and technical scholarship in departments throughout the country. Furthermore, cybersecurity programs are offered at many universities.

In reviewing the annual reports and whitepapers published by the above policing bodies, there seems to be a lack of attention to the financial aspects of cybercrime. While ransomware, extortion, theft, fraud, and cryptojacking are ongoing and emerging concerns (Australian Cyber Security Centre 2017; Australian Security Intelligence Organisation 2018, 2020), there is little indication of where the money taken goes and how criminals launder or cash it out. It is possible – given the view that most attacks happen from an overseas' origin – that there is a lack of domestically-based attackers or illicit merchants (Cunliffe et al. 2017), making it difficult for Australian authorities to pursue cybercrimes back to the offenders and prosecute them unless the offenders have entered and remained within the jurisdiction, and unless the time from offence to pursuit is short.

Financial Crime

Australia is a member of the Financial Action Task Force (FATF) and the Asia Pacific Group (APG). Membership indicates that Australia is compliant or largely compliant in these bodies' recommendations vis-à-vis anti-money laundering and how to combat the financing of terrorism (AML/CFT) (FATF 2018c), though there have been serious problems in regulating the legal profession and in the correct reporting of international financial transfers that have led to serious sanctions by AUSTRAC against major banks 2018-20. Cryptocurrencies are legal in Australia, but they are subjected to money laundering, counter-terrorist financing, and tax laws (The Law Library of Congress 2018). Australia’s principal money laundering intelligence body is:

- **AUSTRAC, the Australian Transaction Reports and Analysis Centre.** AUSTRAC investigates issues related to money laundering and terror finance, among other financial crimes. AUSTRAC notes that cryptocurrencies are used increasingly more today than before and are in need of regulatory oversight in Australia, but there is no indication of their use in criminal acts in its annual report (AUSTRAC 2018a). Anti-money laundering and counter-terrorism financing laws came into force in 2018 to regulate digital currency exchanges operating in Australia (AUSTRAC 2018c). There was no further information available on how cryptocurrencies are used in crime or terror financing. The examples available on AUSTRAC’s website of cybercrime focus on frauds that syphon fiat currency away illegally (AUSTRAC 2018b).

AUSTRAC hosted the first ASEAN Codethon (http://www.austrac.gov.au/codeathon) in Sydney, Australia, in 2018. This event invited industry partners to develop strategies to combat money laundering and terrorist financing that happen in cyber contexts. No written reports of the outcomes or tools developed are publicly available.

Cryptocurrency Regulation

Cryptocurrencies are legal and regulated in Australia; they are subjected to both tax laws and overseen by anti-money laundering and anti-terrorism financing laws. Under Australian law, transacting with cryptocurrencies is a bartering arrangement and has similar tax consequences. Cryptocurrencies may be considered assets for capital gains tax purposes. Cryptocurrencies received for goods or services sold must have their value in Australian dollars recorded and are assessed goods and services tax (GST) on that value at the time of the transaction (The Law Library of Congress 2018; Gainsbury and Blaszczynski 2017).

Australia’s *Anti-Money Laundering and Counter Terrorism Financing Act* (2018) oversees the digital currency exchange providers, subjecting those providers to AML/CFT regulations (Rueckert 2019; FATF 2018d). These regulations require digital exchange providers to verify a customer’s identity before providing services and assessing the AML/CFT risks in “regards to the type of designated service provided, how the designated service(s) will be delivered, the foreign jurisdictions that will be dealt with, and whether the designated service will be offered by a permanent establishment in a foreign jurisdiction” (Irwin and Turner 2018, 302).

Canada

Cybercrime

At the start of the 21st century, Canada viewed cyberthreats as being of low risk; however, by 2015, Canada viewed cybercrime as a serious issue on par with terrorism as a national security threat (Moens, Cushing, and Dowd 2015). Canada has invested millions of dollars domestically and is internationally cooperative (Public Safety Canada 2018). Canada is party to the Budapest Convention and has signed the *Paris Call*. The Canadian government has established a National Cyber Security Strategy, which was last updated in 2018 (Public Safety Canada 2018). Canada treats cyberthreats as multifaceted phenomena that include both cybercrime and other attacks (Adams 2016), and explicitly has interagency efforts in place both domestically and abroad (Deibert 2012). This cooperation provides a wholistic approach in terms of identifying and responding to the entire “script” of a cybercrime, tying criminal activity and its economic implications together.

As is the case in many other jurisdictions, cybercrimes are persisting and increasing in Canada, with DDoS attacks, ransomware, and socially engineered attacks continuing to impact both individuals and businesses (Canadian Internet Registration Authority 2018; Canadian Centre for Cyber Security 2018). Several cybercrime threats are present in Canada, including organised groups that seek to attack underdefended targets, insiders, individual attackers, and hacktivists (Gallagher, McMahon, and Morrow 2014). In addition, cyber espionage has impacted both the government and business sector (Canadian Centre for Cyber Security 2018). Moreover, the Bank of Canada has increased oversight on the Canadian financial market infrastructure (FMI) in response to the continued high risk of attacks upon it (Gallagher, McMahon, and Morrow 2014).

Canada appears to be monitoring a wide array of cybercrimes and is developing mechanisms to support domestic victims and to pursue foreign offenders, where plausible. The Canadian government engages with emerging and ongoing cybercrime-related issues by passing legislation to support investigative and prosecutorial efforts, providing operational support via cyber.gc.ca, conducting events that target various stakeholders in Canada, partnering with private sector actors, and contributing to the capacity building efforts of other countries (Arnold 2018). Of note are agreements with the United States, such as the 2010 Canada-U.S. Action Plan for Critical Infrastructure and the 2012 Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security.

Several government bodies in Canada have cybercrime within their remit, including the Department of Justice, the Royal Canadian Mounted Police (RCMP), Public Safety Canada, and Global Affairs Canada. In addition, there are specific agencies that have specific remits and centres that serve as hubs for the various government actors who collaborate on cybersecurity efforts. These include:

- **Canadian Centre for Cyber Security (Cyber Centre).** The Cyber Centre was established on October 1st, 2018. It serves as a hub where government and private-sector stakeholders can collaborate. The Cyber Centre hosts the National CERT and the Government of Canada CIRT (Computer Incident Response Team) and is responsible for the Get Cyber Safe public awareness campaign. Its website, cyber.gc.ca, provides publicly available information, such as advisories and threat assessments, and tools, such as *Assemblyline*, a malware detection and analysis tool. The website also has a platform where one can report a large variety of cybercrimes and pursue help in the case of victimization. There is a planned **National Cybercrime Coordination Unit** to be run by the RCMP, but it has yet to be formed (Public Safety Canada 2018). The RCMP plays a role in national security, generally, and runs specialised teams, like the **Critical Infrastructure Intelligence Team.**
- **CSIS, the Canadian Security Intelligence Service.** The CSIS is Canada's primary national intelligence service and is part of Public Safety Canada. It has not produced an annual report since 2016. It has produced a report on cyberthreats on critical infrastructure, which raised concerns over attacks from foreign state (or state-supported) actors (Gendron and Rudner 2012); however, it has not revisited those themes.
- In addition to the government bodies, there is also **CIRA, the Canadian Internet Registration Authority**, which manages the .CA internet domain. CIRA provides cybersecurity services for .CA domains, namely the D-Zone DNS Firewall and the D-Zone Anycast DNS, paid services available for .CA domain holders.

Financial Crime

Canada is a member of FATF and APG. The Mutual Evaluation Report indicates that Canada has good anti-money laundering measures in place, though it still remains vulnerable to money laundering through the real estate sector, virtual currencies, and "white-label" automated teller machines (FATF 2016a). Canadian newspapers have reported that anywhere between 1 to 2 billion Canadian dollars have been laundered through British Columbia, associated with wealthy Chinese peoples' dealings in real estate and casinos (Meissner 2019; Cooper 2019). While Canada does not consider virtual currencies as legal tender, it permits their use to buy and sell goods within Canada. In Ontario, 1 in 10 people own or have owned cryptoassets, primarily Bitcoin and Ether (Ontario Securities Commission 2018). Moreover, Canada's tax laws apply to virtual currency transactions, with virtual currencies defined as commodities (The Law Library of Congress 2018). Canada has been advanced in developing regulation for fintech, generally, but virtual currency regulation has lagged behind industry innovation (Ducas and Wilner 2017). Nonetheless, Canada does treat virtual currencies as "money service businesses" and includes them in its anti-money laundering regulations (The Law Library of Congress 2018). In June 2019, amendments to the Proceeds of Crime and Terrorist Financing Act required crypto exchanges to register as money servicing businesses (MSBs) (Government of Canada 2019). Canada has several bodies that have within their remit the investigation of financial crime. These include:

- **CAFC, the Canadian Anti-Fraud Centre.** CAFC collects information and responds to crimes, such as mass marketing fraud, advance fee fraud, internet fraud, and identification theft. It provides public facing information regarding frauds that frequently impact Canadian citizens. It currently features card-not-present fraud, service scams, extortion scams, and tech support scams as crimes of public interest.
- **FINTRAC, the Financial Transactions and Reports Analysis Centre of Canada.** FINTRAC is Canada's financial intelligence unit; it focuses on money laundering and terrorist financing. Its annual report indicates that there has been an increase in virtual currencies used in the commission of various crimes, including drug dealing and terror financing (FINTRAC 2018). FINTRAC cooperates with various law enforcement bodies both domestically and internationally, creating linkages that facilitate the investigation of the financial elements of crime.
- **Royal Canadian Mounted Police Proceeds of Crime Branch (RCMP Proceeds of Crime Branch).** The RCMP's Proceeds of Crime Branch is responsible for policy development, program planning, program monitoring, and resource allocation in order to separate criminals from the profits of their crimes. Most sections of the Proceeds of Crime Branch are part of the Integrated Proceeds of Crime Initiative that brings together a vast array of investigative parties from various government bodies in order to improve investigative and prosecutorial outcomes.

- **CRA, the Canada Revenue Agency.** The CRA has several compliance programs that respond to suspected cases of tax evasions, fraud, and non-compliance with Canada’s tax laws by those who earn income from illegal activities.
- **Local police force financial crime investigative units.** Several local police departments in major metropolitan areas have financial crime investigative units (e.g. Vancouver Police Department; Toronto Police Service) that serve as the first port of call for people living in those cities to file a complaint. They are staffed to conduct investigations and coordinate with other sections within their police departments and with national law enforcement bodies.

Cryptocurrency Regulation

Cryptocurrencies are legal and regulated in Canada but are explicitly excluded as legal tender. Cryptocurrencies are considered commodities by Canadian laws, which means that the value in fiat currency of the goods sold in a transaction must be reported by the seller for income tax purposes and then is taxed accordingly (Canada Revenue Agency 2019).

Canada also subjects cryptocurrencies to its AML/CFT laws. *Canada’s Proceeds of Crime (Money Laundering) and Terrorist Financing Act* views currency exchanges as money service businesses and regulates them thusly. In addition, the Canadian Securities Administrators (CSA) views initial coin offerings (ICOs), initial token offerings (ITOs), cryptocurrency investment funds, and the cryptocurrency exchanges trading these products as being under the purview of Canadian securities law and regulation (The Law Library of Congress 2018), thereby obligating exchanges to employ know-your-customer (KYC) protocols (Rueckert 2019).

India

Cybercrime

India, with its 390 million internet users, has the second most users in the world after China. It has a low internet penetration rate, though that has been slowly increasing. As internet access and speeds increase, the presence of cybercrime emanating from and cyber victimization within the country are likely to increase (Irons and Ophoff 2016). India and the other BRICS economies – Brazil, Russia, China, and South Africa – “have been concerned about the West’s cyberspace dominance and are seeking to change the status quo by engaging in and fostering new international alliances” (Kshetri 2015, 245); none has signed the *Paris Call*. Since 2013, India has been trying to digitise several services (Kshetri 2016), and the government has attempted to demonetise by withdrawing cash from the economy (Garg and Panchal 2016). India's internet users have the potential to engage in over $50 billion USD in online transactions annually (Sheth et al. 2018). India is a prolific producer of software engineers (Iqbal and Beigh 2017); it is projected to have the most software engineers of any country by 2023 (Rana 2018). However, the quality of IT professionals in India varies greatly and many are unemployed or in jobs that are not related to their field of study (The Economic Times 2018). Cybersecurity as an academic major is not commonly offered in India and information regarding relevant study opportunities is limited.

Despite having a large market, there is little research and public information regarding cybercrime trends in India. The number of new users, many of whom do not engage in good cyber security practices, and the use of low-cost and insecure technologies make India susceptible to cybercrime (Kshetri 2017). Data on reported cybercrimes are available via the National Crime Records Bureau (2017) crime statistics. Those statistics show that total cybercrimes increased steadily from 2014 to 2016. The 2016 statistics show that 48.6% of cybercrime cases in India were for “illegal gain,” 8.6% were motivated by revenge, and 5.6% were related to insulting the modesty of women (National Crime Records Bureau 2017). Illegal gain includes crimes such as cyber fraud and forgery (Kandpal and Singh 2013), though what other actions it might include is unclear. Research suggests that the majority of victims of cybercrimes in India are women (Halder and Jaishankar 2016). Estimates of victims of cybercrimes in India indicate that 41 million Indians fell victim in 2011 (Kshetri 2017); however, reported and registered cybercrimes are certainly a small proportion of all cybercrimes that are committed in India (Kshetri 2016). Indian businesses are starting to invest more in cybersecurity measures, amid reports of corporate espionage, ransomware, phishing, and other targeted attacks (KPMG 2017).

India also has a history of generating cybercrime outward to the international market. Spam, fraud, phishing, and crimes with a degree of social engineering, are common (Kshetri 2017, 2015).

India is not party to the Budapest Convention, and, despite having promulgated the Information Technology Act in 2000 and updating it in 2008 (Kshetri 2015), India appears to lack robust and up-to-date regulation to meet the changing demands of online activities and to confront the wide array of frauds that have occurred in India (Nappinai 2010; Umarhathab, Rao, and Jaishankar 2009). Information regarding the degree to which India coordinates with other countries in cybersecurity and cybercrime enforcement is limited. There is some indication that India is using public-private partnerships to improve its capacity (Godse 2016); however, those partnerships are not necessarily valued by government officials (Kshetri 2016). None of the bodies charged with investigating or policing cybercrime produces publicly available reports of any kind. Those groups include:

- **MHA, the Ministry of Home Affairs.** The MHA has a public facing portal (cybercrime.gov.in) to allow the public to report cybercrimes. It caters specifically to “complaints pertaining to online Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content” (Ministry of Home Affairs 2019). The MHA also has a **Cyber and Information Security (C&IS) Division** that is tasked with various coordination efforts among law enforcement agencies and with engaging in law enforcement activity responding to cybercrime.
- **NCSSS, the National Cyber Safety and Security Standards.** The NCSSS is tasked with protecting India against foreign cyberattacks by developing protective technologies, conducting threat assessments, and analysing government, military, and civilian computer networks.
- **NIC-CERT, the National Informatics Centre - Computer Emergency Response Team.** NIC-CERT monitors and responds to cyberthreats to critical government infrastructure. It has a reporting phone number and email. It also publishes advisories and policy guidelines. It is reported that NIC-CERT also runs the **National Cyber Coordination Centre (NCCC),** an e-surveillance agency (The Economic Times 2017). The NCCC, however, is not mentioned on any government website nor does it have its own website.
- **DEITY, the Department of Electronics and Information Technology** is a branch of the Ministry of Electronics & Information Technology. It funds projects to be undertaken by academia. A list of the projects is available, but none of the reports is public.
- There are also **Cybercrime Cells** situated in police departments of most major cities in India and these are tasked to investigate a broad array of cases (Kandpal and Singh 2013).

Financial Crime

India is a member of FATF, APG, and the Eurasian Group (EAG). As is the case with information regarding cybercrime, the government does not produce much publicly available information on money laundering. In 2013, India demonstrated that it was complying well enough with the FATF recommendations to be removed from the annual monitoring process (FATF 2018a); it has remained out of monitoring since then. Nonetheless, India remains a financial hub for the sub-continent (Narayan 2018). Historically, it has experienced large volumes of transactions from remittances that are often remitted using the hawala system (Shehu 2004), though these may be challenged with demonetization (Shirley 2017). However, India has not become a cashless society; two years after demonetization, cash use rebounded to pre-demonetization levels (Dubey 2018). India continues to promote cashless payment solutions, so monitoring the vulnerabilities such systems present is important.

India does not recognise cryptocurrencies as legal tender and does not have a regulatory framework for them[3] (The Law Library of Congress 2018). Indian lawmakers have drafted a bill entitled “Banning of Cryptocurrencies and Regulation of Official Digital Currencies Bill 2019,” published on July 23rd, 2019. From June of 2018, the Reserve Bank of India (RBI) stopped financial institutions from providing services to people or businesses that deal in virtual currencies (Reserve Bank of India 2018). India has suggested that it may develop a Rupee-backed cryptocurrency; however, that project is on hold (Department of Economic Affairs: Ministry of Finance 2019).

India has the following law enforcement bodies tasked with investigating financial crimes:

- **FIU-IND, the Financial Intelligence Unit India.** The FIU-IND is part of the **Ministry of Finance.** Its mission is to combat and deter money laundering and the financing of terrorism. Its annual report states that the FIU-IND has worked with foreign counterparts in these matters and has vastly improved capacity (Financial Intelligence Unit-India 2018). There is, however, little indication of the volume of money laundering in India.

- **Directorate General of Income Tax (Intelligence & Criminal Investigation)** investigates cases of tax evasion. It does not publish any publicly available materials.

Cryptocurrency Regulation

Though India has been attempting to increase its virtual footprint and capacity, it has sought to maintain control over currency by restricting transactions to fiat currency (KPMG 2017). While the Reserve Bank of India (RBI) has approved the use of mobile payment systems, allowing them to exist under the regulation of existing AML/CTF regulation (Reaves et al. 2017), the RBI issued a April 2018 notification that prohibited banks, lenders, and other regulated financial institutions from using virtual currencies (Reserve Bank of India 2018). This prohibition has resulted in a sharp decline in the use of virtual currencies in India. Nonetheless, some companies have challenged the RBI’s directive, and the case is being heard presently in the Indian Supreme Court.

Nigeria

Cybercrime

Nigeria is a country associated with high rates of cybercrime origin. European Union law enforcement views Nigeria as a top-10 country in terms of the location of offenders or infrastructure related to cybercrime (Europol 2015); Symantec views it as the fourth largest producer of cyberattacks in Africa after South Africa, Egypt, and Kenya (Symantec 2016). Nigerian cyber offenders particularly perpetrate various types of fraud (INTERPOL 2018h). As an emerging economy, there are several elements that appear to contribute to Nigeria’s fertility as a location from which cybercrime can occur, including unemployment, cross-border mobility with neighbours, and novice users who do not use basic cyber-wellbeing precautions.

Nigeria experiences an ongoing problem with unemployment (Akanle, Adesina, and Akarah 2016). National unemployment at the close of 2018 was over 23%, a figure that has been steadily high or increasing for at least four years; youth unemployment is higher, with estimates placing it over 30% overall and up to 58% among young women and young people in rural settings (Akande 2014; National Bureau of Statistics 2018). The lack of licit employment opportunities has led to the development of the “yahoo-yahoo” or “yahoo boys” phenomenon. Yahoo boys are typically students in tertiary education who engage in cybercrimes that use social engineering in order to scam victims from overseas (Okeshola and Adeta 2013; Tade 2013). Some of them may also use elements of voodoo as part of their crime ritual (Whitty and Ng 2017; Tade 2013). Notably, these offenders may be part of the Nigerian diaspora, operating in locations outside Nigeria (Kshetri 2016; Whitty and Ng 2017).

INTERPOL indicates that Nigeria is a hub to a broad array of socially engineered frauds and scams (INTERPOL 2018h), with the “business email compromise” scam, whereby scammers spoof high-ranking company officials (Symantec 2016). These frauds generally involve offenders manipulating their victims to transfer fiat currency using remittance systems commonly used by the diaspora to remit money back to Africa (INTERPOL 2018c; Aransiola and Asindemade 2011; Chawki 2009). Changes in banking and transacting in West Africa generally have made tracing financial cross-border transactions more difficult (INTERPOL 2018h). Moreover, the transition to cashless payment systems failed to provide adequate consumer protections; users were victimised by scammers engineering frauds with the new technology and by scammers engaging in fraudulent ATM withdrawals since cashless payment became a widespread option in 2014 (Ukpong and Uke 2016; Tade and Adeniyi 2016, 2017).

Victimization from malware is also common in Nigeria where more than one in seven mobile devices are infected with mobile malware (Symantec 2016). However, there is no clear indication that Nigerian cybercriminals engage in ransomware/extortion activities that would yield cryptocurrency payments. Cryptocurrencies remain legal in Nigeria and several exchanges trade in various cryptocurrencies. Nonetheless, the Central Bank of Nigeria has prohibited banks from transacting in cryptocurrencies, declaring that they are not legal tender (Central Bank of Nigeria 2018), but that regulation does not prohibit the operation of cryptobusinesses, like cryptocurrency exchanges, from operating or banks and financial institutions from investing in them. The Central Bank of Nigeria appears to be developing regulatory policy for fintech companies (Kazeem 2018), though it has stated that, like the internet, cryptocurrency use cannot be banned outright (Chohan 2017).

Nigeria recognises the role its cybercriminals play internationally. It is an observer to the Budapest Convention, but did not sign the *Paris Call*. Nigeria has also passed anti-cybercrime legislation, the Cybercrime Act, 2015 (Mohammed, Mohammed, and Solanke 2019). However, Nigeria appears to be severely under-resourced in terms of being able to cope with cybercrime and financial crime investigations (INTERPOL 2018h; Omodunbi et al. 2016), making it fertile ground for offenders and a place where the increasingly online population may find itself at risk of being victimised from domestic or regional offenders.

Information on Nigerian law enforcement is limited from the country itself. For instance, Nigeria has a National Intelligence Agency, but the organization does not have a working website. Nigeria does have cybersecurity policy and strategy – the National Cyber Security Policy and National Cyber Security Strategy – established in May 2015 (Symantec 2016). Nigeria also has dedicated organizations for cybercrime which include:

- **ngCERT, The Nigeria Computer Emergence Response Team.** ngCERT’s website provides basic information to the public and serves as a portal for reporting cybercrime incidents. The website states that its three principal services are to monitor new technical developments in IT, specifically as they relate to intruder activities; to provide intrusion detection services to information systems that are part of the Nigerian Government’s Critical National Information Infrastructure; and to

engage in vulnerability assessment and penetration testing to private and public entities that are part of the Critical National Information Infrastructure. ngCERT does not produce publicly available whitepapers or reports that provide details regarding the rates of complaints it receives or any further information regarding cybercrime in Nigeria.
- In addition, Nigeria had established the **Nigerian Cybercrime Working Group (NCWG)** with a public outreach mission (Chawki 2009); no website exists for it anymore.

Nigeria has also cooperated with regional and private partners to investigate cybercrime that goes through the country, such as botnet attacks which take control of computers, and to build local capacity (Symantec 2016). There is no indication of the extent to which Nigeria has local training to develop personnel to respond to cybercrime and cyberthreats either through ad hoc education or through trade schools or universities.

Financial Crime

Nigeria emerged from the FATF monitoring process in 2013, indicating that it had improved its AML/CFT regime (FATF 2013). Nigeria is not a member of the Financial Action Task Force (FATF) – South Africa is the only African country that is - but it is a member of GIABA, the Intergovernmental Action Group against Money Laundering in West Africa. The last mutual evaluation report by GIABA on Nigeria is from 2015. It notes that the EFCC is active in investigating and prosecuting local crimes and interfacing with regional counterparts. The report further states that Nigeria is still non-compliant or partially compliant with several AML/CFT policies, including freezing, seizing, and confiscating proceeds of crime (GIABA 2015). The body tasked with investigating is:

- **EFCC, the Economic and Financial Crimes Commission.** The EFCC was founded in 2004 as an anti-corruption agency but also had within its remit the tasks of “preventing, investigating, prosecuting, and penalizing financial and economic crimes such as illegal oil bunkering, terrorism, capital market fraud, cybercrime, advance fee fraud (419 or obtaining through different fraudulent schemes), banking fraud and economic governance fraud (transparence (*sic*) and accountability)” (Obuah 2010). In 2005, the EFCC established the Nigerian Financial Intelligence Unit to collect suspicious transactions reports. Annual reports and further information are not available, but the EFCC does publicise its successful law enforcement activities. Relationships between the EFCC and the government are often tense because some investigations and non-investigations relate to high level governmental corruption. Economic crimes that are independent of elite government-military networks are more freely investigable, but still demand their “proper share” of scarce resources. African scholars suggest that the EFCC remains under-resourced and local confidence in its efficacy appears to be limited (Suleiman, Othman, and Ahmi 2017; Uthman et al. 2015). Interviews with officials (personal communication) suggest that the EFCC does investigate 419 fraud gangs who use electronic communications and receive wire transfers as well as cash as part of their operations.

Cryptocurrency Regulation

Though Nigeria has one of the highest rates of cryptocurrency usage in Africa, it is not the topic of much outside inquiry. Cryptocurrency can be traded in Nigeria, but the Central Bank of Nigeria (CBN) states that cryptocurrencies are not legal tender and that virtual currency exchangers (VCEs) are not licensed or regulated by the CBN. However, cryptocurrencies are not barred; rather, Nigeria’s Securities and Exchange Commission states that those who trade in cryptocurrency must do so at their own risk (Oyebayo and Shittu 2018). Nonetheless, the CBN requires Nigerian financial institutions that engage with VCEs to ensure that the VCEs comply with *the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Regulations*, 2013, and *The Nigerian Cyber Crime (Prohibition, Prevention) Act,* 2015. These regulations and statutes require Nigerian financial institutions to follow KYC protocols and report suspicious transactions to the Nigerian Financial Intelligence Unit (NFIU) (Oyebayo and Shittu 2018; Sanni 2019).

South Africa

Cybercrime

South Africa, despite an internet penetration rate of only about 53% (Symantec 2016), was the top source of cyberattacks on the African continent, accounting for 25% of all attacks (Symantec 2016). It was the top source for malware, spam, and phishing hosts; fourth for botnets; and second for hosting C&C (command and control) servers. It also ranks high in terms of victims, ranking third in the world, behind China and Russia, in 2013 (Kshetri 2015), resulting in losses of over $300,000,000 USD annually (Irons and Ophoff 2016). In addition, some cybercrime may be targeted for political purposes (Van Niekerk 2017). These high rates in terms of Africa could be attributed, at least in part, to the early access South Africa has had to broadband connections relative to the rest of the continent and to an overall lack of security awareness (Irons and Ophoff

2016; Bada, Von Solms, and Agrafiotis 2018). Its relative wealth also has been a magnet for Africans from other countries, including Nigerians.

Collecting up-to-date information on South Africa and cybercrime victimization within it or cybercrime offending emanating from it is variable. Within South Africa, there are no public-facing, accessible reports produced by organizations in the country. Most information related to South Africa’s levels of cybercrime offending and victimization is produced by consultancies working on the topic or by foreign government reports. Consultancy reports tend to focus on issues that these consultancies view as directly relevant to their customer base. Foreign government reports have proved to be irregular. Notably, there are problems in terms of data collection and enforcement capacity in South Africa. Victims of cybercrimes often fail to report crimes since they fail to recognise that they are being victimised; plus, mandatory reporting is not obligated (Van Niekerk 2017). Additionally, poor operational procedures and reporting protocols within businesses are common (Bougaardt and Kyobe 2011). Enforcement lacks sufficient capacity to respond to known threats and to investigate crimes effectively and consistently; nonetheless, South Africa has assisted with mutual legal assistance requests (Symantec 2016; Irons and Ophoff 2016).

INTERPOL recognises that cybercrime assists with an array of other crimes that are common in southern Africa. Technology can facilitate investment and innovation by providing facilities illicit entrepreneurs can use to transfer money, produce counterfeit documents, and communicate across borders and illicit markets (INTERPOL 2018g). Interpol indicates that cybercrimes in southern Africa, therefore, have a degree of sophistication that is less prevalent elsewhere in the continent. Moreover, banks and payment systems are common targets (Bougaardt and Kyobe 2011; Mbelli and Dwolatzky 2016).

South Africa is an observer to the Budapest Convention, but did not sign the *Paris Call*, and has passed some domestic legislation to combat cybercrime. However, as is the case for many African countries, there is a gap between the laws on the books and the ability for law enforcement organizations to enforce them (Kshetri 2013). Moreover, few South African universities offer coverage of cybersecurity issues; none offers a comprehensive program of study in cybersecurity (Irons and Ophoff 2016). Unlike other African countries, South Africa does regulate cryptocurrency, namely through its tax laws which state that individuals must declare cryptocurrency holdings and gains to the South African Revenue Services (SARS) (The Law Library of Congress 2018).

South Africa has several policies and pieces of legislation that focus on cybersecurity (Sutherland 2017). The cornerstone of these policies is the National Cybersecurity Policy Framework (NCPF), passed in 2012 (Department of Telecommunications and Postal Services 2017). In concert, these polices have established or empowered existing bodies to counter cybercrime. Sutherland (2017) provides a chart that shows the relationships between policy departments and agencies. However, the majority of these organizations do not have public facing websites with publicly available information. The following are the organizations that have public facing information:

- **CSIRT, Computer Security Incident Response Team.** The CSIRT is located under the **State Security Agency (SSA)**. It provides ICT and cybersecurity services to the government. It publishes an irregular newsletter, daily ICT information security reports, and security advisories that are publicly available.
- **CSIRTs, Computer Security Incident Response Teams**. In addition to the South African National CSIRT, there are various CSIRTs throughout South Africa. CSIRTs are part of the Department of Telecommunications and Postal Services (DTPS). They have a remit to help protect South African citizens and businesses online. The National CSIRT maintains the National Cybersecurity Hub, which serves as a central point of collaboration between the government and non-governmental partners. The National Cybersecurity Hub has an email where one can report cybersecurity incidents, including phishing, malware, and ITC vulnerabilities.

The National CSIRT has produced a document entitled “A Baseline Study on Cybersecurity Readiness” (Department of Telecommunications and Postal Services 2017). The document reports on readiness as it relates to South African businesses. It states that there are insufficient in-house skills and awareness, and development in these two areas. It also notes that ransomware and malicious emails, and socially engineered attacks remain a significant concern in terms of external threats. However, the report notes that internal threats pose a bigger risk.

> The DTPS also has established a **National Cyber Security Advisory Council;** however, little information is available regarding it.

- **SAPS (South African Police Service) Electronic Crime Unit.** The SAPS Electronic Crime Unit runs cybercrime.org.za which is a portal for resources on cybercrime, such as relevant laws and policies, security tips, and a public portal to report cybercrimes. Reports have indicated that SAPS Electronic Crime Unit is under-resourced, with preventable issues, such as expired software licenses, impeding its ability to function (Sicetsha 2018).

Financial Crime

South Africa has an extremely high rate of financial crime, with 77% of South African organizations having experienced economic crime in some form (PwC 2018b). Fraud, tax crimes, misappropriation crimes, and money laundering appear to have risen recently or remain prevalent in South Africa (PwC 2018b; Financial Intelligence Centre 2018a). Financial crime is associated as an element of other types of serious and organised crime in Southern Africa, generally; criminal organizations exploit the "contrast between informal economies and sophisticated and developed complex financial infrastructure spread throughout the region" (INTERPOL 2018g). Overall, financial crime costs the region billions of dollars and stunts its ability to develop and grow (INTERPOL 2018g; PwC 2018b).

These high rates and ongoing phenomena are despite the presence of legislation that seeks to combat financial crime (de Koker 2007, 2003; Financial Intelligence Centre 2018a) and membership to **FATF** and the **Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)**, indicating a lack of capacity which is common throughout the region (INTERPOL 2018g). Nevertheless, the most recent mutual evaluation review of South Africa by FATF/ESAAMLG states that South Africa has made progress in terms of complying with the regulatory suggestions (ESAAMLG 2018). The organization tasked with combatting financial crime in South Africa is:

- **FIC, the Financial Intelligence Centre**. The FIC was established in 2003 with a remit to gather and analyse financial data (Financial Intelligence Centre 2018c). It currently works on financial crime broadly and engages in anti-money laundering and anti-terror financing efforts (Financial Intelligence Centre 2018a). In addition to annual reports, the FIC publishes regular updates on scam types, illustrating common scams that impact South Africa.

Recent publications have highlighted fraud related to cryptocurrencies and other virtual assets, credential theft, bank fraud, socially engineered frauds, and unauthorised use of third-party accounts (Financial Intelligence Centre 2018c, 2018b). Overall, the FIC demonstrates an awareness of the nexus between cybercrime and financial crime and appears to be moving towards developing policy and producing information that address this specific issue (Financial Intelligence Centre 2018a).

Cryptocurrency Regulation

Cryptocurrency is largely unregulated in South Africa. Upon review, the South African Reserve Bank determined that virtual currencies, including cryptocurrencies and digital currencies traded within video games, are not legal tender; nonetheless, cryptocurrencies are subject to taxation upon their transaction (South African Reserve Bank 2014; The Law Library of Congress 2018). South Africa also requires financial virtual exchanges to report suspicious activity (FATF 2018d).

United Kingdom

Cybercrime

The United Kingdom is one of the most-often-targeted countries by cybercriminals, with offenders being of both a domestic and an international provenance (Saunders 2017, NCA 2020). Cybercrime is a most common type of crime experienced in the United Kingdom, with 1 in 12 reported crimes relating to computer misuse (Crime in England and Wales: Additional Tables on Fraud and Cybercrime 2020; Budd 2016). It is in the top 10 of countries where ransomware is most prevalent (Symantec 2017). In 2018, victims of cybercrime in the United Kingdom lost more than £190,000 daily (Lee 2019); in 2020, cybercrime increased 5% from 2019 (ONS 2020).

Domestically, the United Kingdom’s organization of law enforcement has grown historically but not always tightly or coherently; this is also true in terms of law enforcement and cybercrime investigations, regularly criticised in HMICFRS reports. That being said, the UK Government (2016) published its *National Cyber Security Strategy 2016-2021*. This report highlights the ongoing threats domestically and abroad and outlines the government strategy to “defend, deter, and develop,” punctuated by a £1.9-billion investment in cybersecurity (HM Government 2016). Security strategies propose (and have precipitated in) the development of public-private partnerships to improve capacity (Saunders 2017; Budd 2016). Domestic organizations that focus on cybercrime are:

- **NCA, the National Crime Agency.** The NCA is responsible for tackling the most serious international organised crime and for cyber dependent (but not cyber-enabled) crime, including child sexual exploitation, money laundering and illicit finance, data breaches, ransomware attacks, and distributed denial of service attacks. The associated regional organised crime units (ROCUs) are semi-independent and sometimes conduct specialist surveillance and cybercrime investigations, some of which have involved cryptocurrencies.
- **GCHQ, the Government Communications Headquarters.** GCHQ is the United Kingdom’s signals intelligence branch. The **National Cyber Security Centre (NCSC) is part of GCHQ and the UK’s lead technical authority on cyber**

> **security. It offers real-time threat analysis, defence against national cyber attacks and tailored advice to small and medium enterprises, large organisations, the public sector and the general public on improving cyber resilience and responding to incidents. It works collaboratively with law enforcement, defence partners, the UK's intelligence and security agencies and international allies. The NCSC also provides certification to cyber security products, services and organisations, and relevant training and degree programmes.**

Additionally, GCHQ has a private-public partnership with the **P20 Collaborative (**https://payments20.com/**)** an organization that represents corporations wishing to promote collaboration on a variety of topics, such as financial inclusion, technology and platform development, as well as cybersecurity. P20's cybersecurity working group produces research and recommendations on the mitigation of cyber risk. In addition to its relationship with GCHQ, P20 has ongoing dialogue with the U.S. Department of Homeland Security and Department of Justice.

Internationally, the United Kingdom is a party to the Budapest Convention and has signed the *Paris Call*. As a member of the European Union, it has contributed to investigations and to the work of the European Union Agency for Network and Information Security (ENISA), whose role has been upgraded in recent years to reflect the ascent of the issues within the EU's crime and enterprise portfolios. However, post-Brexit there is a likelihood of increased risk to the United Kingdom, as its agencies will no longer enjoy the same degree of support from partnering institutions in the European Union, foreign talent may leave, and the general capacity lull will be a scenario that attackers will seek to target. Likewise, the capacity of Europol and EU Member States will be diminished.

Financial Crime

Financial crime comprises two interconnected but connected strands: fraud and money laundering. Much fraud is laundered (in the formal sense), but money laundering applies to the proceeds of all domestic and overseas crimes. The United Kingdom is not only the largest financial service provider in the world but also possesses the highest rating of any FATF-assessed country in the latest round of assessments (FATF 2018b). It is, likewise, home to the largest centre for financial payments: $9 trillion USD in financial payments pass through London's 210 FinTech companies. In the UK, 50% of corporate respondents reported experiencing economic crime in the past 24 months, a figure which is comparable to the global average of 49% (PwC 2018a).

Fraud accounts for about a third of all crime reported and that money laundering may exceed £90 billion a year, though those estimates are often contested (HO News Team 2017; Moiseienko and Keatinge 2019). The financial sector reports a prevalence of several cyber-enabled frauds, including identity fraud/theft, phishing, unauthorised access, and malware-enabled fraud (Financial Conduct Authority 2018; PwC 2018a).

Cryptocurrencies are legal in the United Kingdom. In the past, the government position has been that the size of the market is too small to regulate, but the Bank of England has called for regulation (The Law Library of Congress 2018). There are some self-regulating bodies in the crypto-asset industry, such as Crypto UK, and by the **Financial Conduct Authority (FCA),** the UK's financial services regulator (House of Commons Treasury Committee 2018). In 2020, FCA called for businesses carrying on cryptoasset activity in the UK to come into compliance with *the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017*, as amended in 2019 (MLRs) and to register with the FCA (Levi and Gelemerova, 2020).

The United Kingdom is a member of FATF and the latest mutual evaluation report notes that it has a robust understanding of money laundering and terror financing risks and has a good record for prosecuting high-end money laundering cases and cooperating with foreign counterparts (FATF 2018b). Although FATF notes that the UK generally has good information for investigative purposes, it recommends "an overhaul to improve the quality of financial intelligence available to the competent authorities" (FATF 2018b, 4), which has begun. Principal domestic bodies concerned with financial crime include:

- **SFO, the Serious Fraud Office.** The SFO is responsible for some of the most serious economic crimes, including transnational bribery, but (per researcher interviews) the SFO rarely detects cryptocurrencies in its investigations. This is understandable because the businesses investigated are mostly businesses trading licitly or apparently licitly, so those businesses would normally use financial transactions appropriate to their kind of business. There is little evidence of crypto currencies being involved in transnational bribery, though such evidence may take time to emerge in enquiries that are generally of long duration. One recent study of kleptocratic behaviour (Sharman 2017) makes no mention of crypto currencies.
- **City of London Police, Economic Crime Department.** The City of London police economic crime **department** is the official lead agency for economic crimes in

England and Wales, including cyber enabled economic crimes. It does sometimes deal with cases involving cryptocurrencies.

- **UK Financial Intelligence Unit.** The UK Financial Intelligence Unit is part of the **NCA.** It is the body responsible for processing Suspicious Activity Reports (SARs), investigating them, or passing on the SARs to appropriate bodies.
- **Action Fraud and the National Fraud Intelligence Bureau.** Action Fraud and the National Fraud Intelligence Bureau are the bodies to which frauds are reported centrally and which process these reports before passing them on. There are no reports which specifically mention cryptocurrencies, but frauds involving exchanges may be investigated. Action Fraud also serves as a portal where members of the public can report frauds and scams.
- **National Economic Crime Centre (NECC).** The NECC is the central coordinating body established in 2018 within the National Crime Agency. The NECC seeks to coordinate the UK’s response to economic crime; this includes the use of cryptocurrency to launder the proceeds of crime or to transfer illicit funds. It is too early to state what its role is or is likely to become in relation to cryptocurrency laundering. The theft of cryptocurrency values from exchanges may become the subject of an economic crime investigation by any of the above bodies. The NECC is establishing public-private partnerships to prevent economic crime, but cryptocurrencies are just one among many sources of harm, whether as laundering media or as objects of fraud from licit and illicit users.

Cryptocurrency Regulation

The United Kingdom regulates cryptocurrencies via the tax code and (as is the case with all EU countries) under the Fifth Money Laundering Directive (5AMLD). Under UK tax law, “corporations pay corporate tax, unincorporated businesses pay income tax, individuals pay capital gains tax” (The Law Library of Congress 2018, 3). The UK Gambling Commission views digital currencies as not constituting real money gambling (Gainsbury and Blaszczynski 2017), though this ruling does not obviate the need for AML regulation. In accordance with 5AMLD, the UK regulates virtual currency exchanges and custodian wallet providers (Moiseienko and Kraft 2018). Overseeing this task is HM Treasury-Financial Conduct Authority-Bank of England Cryptoassets Taskforce, which assessed the potential risks and benefits of cryptocurrency and the underlying distributed ledger technology, and set out the UK’s policy and regulatory approach which seeks to protect consumers and markets from risk and to curb the use of cryptocurrency for illicit activity (HM Treasury 2019).

United States

Cybercrime

The United States is, by some estimates, the country with the highest number of both offenders and victims in terms of cyberattacks and cybercrime (Akamai 2019; Symantec 2017). Moreover, the US's position as a world political power, status as a leader in communications and military technology, and central position as a financial world hub, make it an attractive target for state and non-state actors. At an international level, the US is a party to the Budapest Convention but, notably, refused to sign the *Paris Call*, joining countries that have been associated with state-sponsored cybercrime and cyberattacks (Matsakis 2018).

Media coverage has recently focused on foreign interference in US elections (Hennessey 2017), but a wide array of serious vulnerabilities exist at the state and municipal levels, where cash-strapped and ill-prepared governments have been successfully targeted in ransomware schemes, and where voting infrastructure has been targeted by foreign actors. In the US, the greatest imminent security threats have been identified as arising from the proliferation of IoT devices (e.g., home-based systems associated with Amazon, Apple, and Google) and the rapid adoption of cloud computing without concomitant appropriation of up-to-date security. Several vulnerabilities persist. Significant vulnerabilities targeted by state and non-state actors are within:

- military infrastructure, including, *inter alia*, the Pentagon, the Department of Homeland Security, and US intelligence agencies (Clapper et al. 2017; Lindsay, Cheung, and Reveron 2015);
- the national, critical infrastructure grids, such as power, communication, and transportation and aviation (Carter and Sofio 2017; Baggett and Simpkins 2018; T.A. Johnson 2015b; Clark and Hakim 2016), which may be affected by cyberespionage, which has been an ongoing issue (Laszka et al. 2014; Lindsay, Cheung, and Reveron 2015; Lubold and Volz 2019);
- corporate entities, including Fortune 500 companies, particularly those in the "fintech" sector, such as the payments industry, credit card companies, and banks (K.N. Johnson 2015a; Bouveret 2018);
- supply chains, which saw a 78% increase in attacks in 2018 (Symantec 2019); and
- public-private partnerships (M. Carr 2016), particularly those that provide services to government infrastructure, such as the cloud hosting of government sites.

Additionally, commonplace cybercriminal events and the investment to protect against them persist and cost the US economy an estimated $57 to $109 billion dollars in 2016 (The Council of Economic Advisers 2018). Cybercrime victimization in the US is experienced both at the individual and company level (The Council of Economic Advisers 2018). One in four Americans has experienced cybercrime on the individual level (Reinhart 2018). American businesses have been increasing their spending on prevention and response consistently over the past five years as cybercriminals become more efficient in scaling their criminal capacity (Pomemon Institute 2017). Despite these high costs, there is a cyber enforcement gap; attackers are subjected to law-enforcement action in less than 1% of malicious cyber incidents (Eoyang et al. 2018).

Contributing to the complexity of cybercrime enforcement is the fact that the US is a federated system, with many states and municipal government authorities responsible for their own defence, investigation, and interdiction systems. Accordingly, cybersecurity investigations can be uncoordinated and under-resourced (Eoyang et al. 2018). In an effort to make up the law-enforcement shortfall, US cyber infrastructure is heavily entwined with private information technology (IT) and information system (IS) infrastructure through public-private partnerships (Ballou, Allen, and Francis 2016). There exists a National Cyber Strategy, released by the Trump Administration in 2018, that focuses on national cyber-security threats. The 26-page report emphasizes a “best defense is offense” strategy (The Executive Office of the President 2018). It outlines a plan to provide government agencies with more powers to proactively fight cybercrime (e.g., counter-hacking) and emphasizes greater cooperation with private companies, including multinationals that do business in countries involved with cyber-related dispute or crimes in the U.S (e.g., China and Russia).

In the US, there are cybercrime investigative bodies, task forces, and legislated partnerships between federal agencies – such as the **Department of Defense** and the **Department of Homeland Security** – that share similar concerns and resolve in combating cybercrime. These include:

- **FBI, the Federal Bureau of Investigation.** The FBI is the lead federal agency for investigating cyber-attacks by state and non-state actors, with a focus on counterterrorism and counterespionage. Additionally, the FBI has developed technological and investigative capabilities and partnerships that include teams and squads present at the FBI headquarters and in each of the FBI’s 56 field offices that deal with a broad array of cybercrimes, including computer intrusions, data theft, online fraud, and the production of child exploitation materials.

The FBI runs the **Internet Crime Complaint Center (IC3)**, which is a public-facing information and cybercrime complaint portal. The IC3 produces an annual report on the state of cybercrime affecting the United States, presenting crime breakdowns by cost, type, and state (FBI 2018).

Additionally, the FBI manages **iGuardian**, a secure information portal allowing industry-based, individual partners to report cyber intrusion incidents in real time. The iGuardian portal is an evolution of **eGuardian,** a sensitive-but-unclassified (SBU) information-sharing platform hosted by the FBI's Criminal Justice Information Services (CJIS) division as a service on the Law Enforcement Enterprise Portal (LEEP). iGuardian went beyond law enforcement users and was developed specifically for partners within critical telecommunications, defence, banking and finance, and energy infrastructure sectors. It is available over the SBU InfraGard network.

- **NCIJTF, the National Cyber Investigative Joint Task Force**: The NCIJTF, established in 2008, is comprised of over 20 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organization's mission of coordinating cyber threat/cybercrime investigations of crimes, including fraud, espionage, identity theft, and terrorism, from a whole-of-government perspective.

- **DHS, the Department of Homeland Security.** The DHS is the agency in charge of domestic security. The DHS houses **CISA, the Cybersecurity and Infrastructure Security Agency.** The CISA helps organizations manage risk and provides access to resources to maximise this risk management. The DHS runs **NCCIC, the National Cybersecurity and Communications Integration Center**, a hub that facilitates information exchanges regarding cyber defence and incident response. It is comprised of what were the NCS, National Communications System; NCC, National Coordinating Center for communications; US-CERT – United States Computer Emergency Readiness Team, and ICS-CERT, Industrial Control Systems Cyber Emergency Response Team. Also housed in the DHS is **ICE, the Immigration and Customs Enforcement,** which houses **C3, the Cyber Crimes Center**. C3, established in 1997, deals with trans-border criminal investigations of Internet-related crimes within the Homeland Security Investigation's (HSI) portfolio of immigration and customs authorities. C3 is responsible for identifying and targeting any cybercrime activity in which HSI has jurisdiction. It has three subdivisions:

  - **CCU, the Cyber Crimes Unit.** The CCU is responsible for developing and coordinating investigations of immigration and customs violations where the criminal act is facilitated by use of the internet. Crimes that fall under the CCU's remit include financial fraud, money laundering, identity and benefit fraud, the sale and distribution of narcotics and other controlled substances, illegal arms trafficking, and the illegal export of strategic/controlled commodities.
  - **CEIU, the Child Exploitation Investigations Unit.** The CEIU is responsible for the Child Exploitation Program within the Homeland Security Investigation portfolio.
  - **CFU, the Computer Forensics Unit.** CFU manages **the Computer Forensics Laboratory** and provides programmatic oversight, equipment, technical support, training, and guidance for the ICE Computer Forensics Program (CFP).
- **CCIPS, Department of Justice, Computer Crime and Intellectual Property Section.** CCIPS implements the Department of Justice's national strategies in combating computer and intellectual property crimes. CCIPS prevents, investigates, and prosecutes computer crimes by cooperating with other US government agencies, the private sector, academic institutions, and foreign counterparts.

Financial Crime

The United States is a member of FATF and APG. While the US has a robust AML/CFT framework that oversees coordination and cooperation across several domestic law enforcement bodies, the US still has significant gaps in its regulatory frameworks for businesses associated with financial and property advisors and agents (FATF 2016b), particularly as some of these sectors have ongoing self-regulation regimes (Jakobi 2018). The US is especially at risk of having money laundering events happen through its banks, given the global volume of the US dollar that results in trillions of dollars of daily transaction volume through US banks (FATF 2016b). The city of Atlanta, the US payments industry capital, sees $6 trillion US dollars pass through it annually in terms of financial payments. It appears that most of the AML efforts focus on comparatively large payments; there is a lack of predicate tax crimes that facilitate more efficient prosecution of money laundering more broadly (FATF 2016b). The FBI has produced reports on financial crimes but has not done so since 2011. Primary law enforcement bodies that deal with financial crimes in their remit are:

- **FinCEN, Financial Crimes Enforcement Network.** FinCEN is a bureau of **the United States Department of the Treasury** that serves as the US financial

intelligence unit. It collects and analyses information about financial transactions in order to combat domestic and international money laundering, terrorist financing, and other financial crimes. FinCEN produces advisories to industry actors on the issues of financial crime, money laundering, and terror financing.
- **IRS (Internal Revenue Service) Criminal Enforcement.** The IRS Criminal Enforcement division investigates alleged violations of the Internal Revenue Code, the Bank Secrecy Act, and various money laundering statutes. It monitors issues related to counterterrorism, with particular focus on computer forensics and dark web transmission of funding. IRS Criminal Enforcement also actively participates in high-level espionage investigations, with newfound emphasis on cybersecurity and private industry partnerships to ensure the federal tax system is not being misused or targeted by state or non-state actors. However, budget cuts enacted by Congress since 2011 have left the IRS perpetually underfunded, meaning that its capacity to investigate financial crimes effectively and consistently has been curbed.

Cryptocurrency is legal in the United States. The FBI recognises cryptocurrency's role in crime: the IC3 reported over $58 million in losses in cryptocurrency (FBI 2018). There has been confusion as to which regulatory bodies have oversight and the responsibility to enforce the law in relation to cryptocurrencies due to confusion on whether cryptocurrencies should be classified as securities, commodities, or payments (Blumenfeld et al. 2018). There are currently two bodies taking the lead in terms of cryptocurrency oversight. These are:

- **SEC, the US Securities and Exchange Commission.** The SEC's mission is to protect investors, maintain fair, orderly and efficient markets, and facilitate capital formation. The SEC coordinates with the Department of Justice to investigate various types of fraud. The SEC set up a **Cyber Unit** to target cyber-related misconduct that involves the manipulation of virtual assets and the theft of non-public information that could influence buying and selling behaviour. It is now organizing investigations of "pump-and-dump" schemes associated with the $400 billion cryptocurrency market, including a number of coordinated international investigations with other countries to stem the use of cryptocurrency ghost exchanges designed to steal funds and fund criminal activities (Clayton 2017).
- **CFTC, the US Commodity Futures Trading Commission.** The CFTC's mission is to foster open, transparent, competitive, and financially sound markets. To achieve these objectives, the CFTC provides oversight on markets (e.g. the futures market and swaps market), industries, and individuals within its purview and helps facilitate investigations of crimes within these spaces. It provides publicly available

information about the futures and swaps markets, issues opinions and adjudicatory orders on administrative enforcement cases, and contributes to investigations that centre on illicit transactions, including money laundering. Some cryptocurrency clearing houses and exchanges are registered with the CFTC, and the CFTC views cryptocurrency as commodities subject to its oversight. It provides information on its website (https://www.cftc.gov/Bitcoin/index.htm) for consumers, regarding virtual currencies, risks related to investing in them, along with information related to markets where cryptocurrencies may be traded.

Cryptocurrency Regulation

Cryptocurrencies are regulated in the United States. Exchanges and other platforms that trade in virtual currencies must register as money services businesses or money transmitters per the *US PATRIOT Act* (Brito 2014), thus subjecting them to AML/CTF rules that require KYC protocols and reporting large and suspect transactions to FinCEN (Moiseienko and Izenman 2019; Forgang 2019; Fein 2018). Cryptocurrency merchants are also subject to the Bank Secrecy Act, which is intended to facilitate the prevention and detection of money laundering and terrorism finance (Brito 2014). The Internal Revenue Service (IRS) treats cryptocurrency as property (Fein 2018); gains from transacting cryptocurrency are taxable and must be reported to the IRS (Burks 2017).

International Bodies

Europol

Europol, being an entity under the European Union, is an observer organization to the Budapest Convention. It is an observer organization to FATF. It has signed the *Paris Call*. Cybercrime is an important issue for Europol and has led to the creation of the **European Cybercrime Centre (EC3)** and the **Joint Cybercrime Action Taskforce.**

The EC3 is comprised of two forensics teams, digital forensics and document forensics, each of which focuses on operational support and research and development. Its law enforcement support activities focus on cyber-dependent crime, online child sexual exploitation, and payment fraud. The EC3 produces a usually annual report called the *Internet Organised Crime Threat Assessment (IOCTA)*, that discusses current cybercrime and cybersecurity threats to, and recent efforts undertaken by, the European Union.

The most recent edition, in 2018, highlights a variety of issues related to crime financing and criminal investigation (EUROPOL 2018). Financially motivated cybercrimes, including the deployment of ransomware, DDoS attacks, card-not-present fraud, and skimming, continue to grow or are done at a sustained rate. Cryptocurrency has been increasingly used in financially motivated crimes. Bitcoin still holds a dominant position in terms of the cryptocurrency that comes under investigation, but other cryptocurrencies are increasing in the market. In addition, there is the trend of cryptojacking, that is the use of cryptomining malware, which involves illegally using a victim’s computer’s bandwidth to mine cryptocurrencies (Pastrana and Suarez-Tangil 2019). Cryptocurrencies are still frequently transacted in illicit darknet forums. Darknet markets still persist and even flourish, despite takedowns of notable marketplaces. The report also notes that cryptocurrency investigation capacity needs to expand.

Together with INTERPOL, Europol hosts an annual conference on cybercrime, where various presenters from law enforcement and industry discuss recent investigations, concepts, and concerns. Europol also maintains a board of experts to provide insight and suggestions from points of view outside law enforcement.

INTERPOL

INTERPOL is an observer organization to the Budapest Convention. It is also an observer organization to FATF, and accordingly it facilitates research, capacity building, and cooperation among member nations in pursuing both cybercrime and financial crime.

Cybercrime is an increasing part of INTERPOL’s research and support portfolio. INTERPOL built its Global Complex for Innovation in Singapore and that space houses the Cyber Fusion Centre, a unit that focuses on cyberthreats, broadly stated (INTERPOL 2018b). The unit is staffed by a multinational and multi-stakeholder team, most of whom are seconded from law enforcement bodies. INTERPOL works on behalf of its member states and facilitates their law enforcement bodies’ capacity to interface with each other. It provides training for law enforcement bodies of member states and has participated in several multinational initiatives. One such initiative is TITANIUM (Tools for the Investigation of Transactions in Underground Markets), which seeks to “reveal common characteristics of criminal transactions, detect anomalies in their usage, and identify money-laundering techniques” (INTERPOL 2018a, 36-37). INTERPOL also has produced a *Global Cybercrime Strategy* that focuses on crimes against computers and information systems with the goal of improving information sharing, threat assessment, and crime attribution (INTERPOL 2018b).

The 2017 annual INTERPOL report flags two points of interest related to cyber-enabled crime. First, there have been improvements in terms of identifying command and control servers that help facilitate crimes, such as phishing operations and ransomware. Second, the African cyber economy in terms of offenders and potential victims is expanding rapidly. This second point is further echoed in the INTERPOL reports on organised crime in Africa (INTERPOL 2018c, 2018d, 2018e, 2018g, 2018h, 2018f), and indicates that there is a great need to research these issues on the continent as well as work towards building capacity within African countries.

Overall, INTERPOL describes Africa as having three problems vis-à-vis cybercrime and financial crime. First, a “lack of investment and awareness [that is] exacerbated by limited capacities to prevent, detect, and investigate cybercrime incidents is further driving this criminality on the continent” (INTERPOL 2018c, 6). Second, there are similar limitations in financial crime control. Third, given that the region’s users are novices, local reporting of crime may be extremely low (INTERPOL 2018d). Moreover, at times, investigations mischaracterise the crimes they report, thus creating an opaque picture of crime in the region (INTERPOL 2018h). The weak financial crimes intelligence presence, coupled with a lack of research on cybercriminal actors in Africa, results in a fertile space for cybercriminals to develop and prosper.

To that end, cyber-enabled crimes, including illegal access of computer systems, fraud, malware attacks, and the trade of prohibited goods and content, will continue to grow with the increased connectivity of the continent’s people (INTERPOL 2018c). Offenders are aware of the regions’ law enforcement deficiencies and may, in cases, use their diaspora networks to operate purposefully across borders and evade detection (INTERPOL 2018c, 2018g). Particularly, there are several, often complex, financial crime schemes that are executed daily across Africa that include banking fraud and breaching financial payment networks (INTERPOL 2018c). INTERPOL suggests, however, that there are some regional trends, in terms of cybercrime and cyber-enabled financial crimes committed and victim types.

In West Africa, INTERPOL has drawn particular attention to two criminal organizations, the yahoo boys and The Next-Level Cybercriminals (INTERPOL 2018a). The Yahoo Boys – identified by African scholars as a sub-culture or cultural phenomenon rather than a fixed group (Akanle, Adesina, and Akarah 2016; Omeire and Omeire 2016) – rely on low-tech fraud schemes, such as advance-fee, stranded traveller, and romance frauds. The Next-Level Cybercriminals have deployed crime-enabling software to conduct more sophisticated attacks. INTERPOL states, more generally, that there is a typical cybercriminal profile: men between 19 and 39, who have developed technological skills. These actors apparently present themselves ostentatiously, with visible indications of their new-found wealth. The report indicates that Nigeria is a "hub for the 'CEO-Fraud' scheme (also known as 'Director-Fraud,' 'Supplier-Fraud,' 'Email Scam') as well as the Business Email Compromise (BEC) scheme" (INTERPOL 2018h, 21), though the scope of these frauds is unclear. It further indicates that Côte d'Ivoire is a hub for sextortion, that mostly targets people living in the Americas and Europe (INTERPOL 2018h).

In terms of financial crime, the report notes that money laundering is facilitated by the large cash-based economy that still dominates most countries in West Africa. Currency is remitted routinely, using a variety of remittance services, which facilitate the transfer of fiat currencies. These systems, coupled with limited law enforcement capabilities, make enforcement difficult. There is no comment regarding non-fiat currency presence in the region, perhaps indicating the prevalence of fiat currency scams.

In East Africa, most cases relate to financial crimes and telephone fraud and are characterised by an increasing degree of hi-tech equipment usage. Money laundering is a crime which is of recognised importance to the region, but a lack of reporting means that no single scheme has been identified as being predominate or emerging. The emergence of alternative payment systems (notably *M-Pesa* in Kenya) that serve the diaspora populations and the emergence of mobile financial systems have changed financial flows from being primarily cash based to digital based. Fourteen per cent of Africans receive money through mobile transfers, thereby leading the world in mobile transfers (Symantec 2016). Apparently, these transactions have a high degree of anonymity (INTERPOL 2018e).

In Central Africa, INTERPOL highlights that hosting services for illicit products (phishing engines, malware) are present. Money laundering operations are present in the region and focus on fiat currencies. Transactions commonly involve the gold or diamond industry; however, estimates that quantify the volume of money laundered are not available (INTERPOL 2018d).

In Southern Africa, cybercrime has facilitated transnational organised criminal activities that victimise people within the region and further afield, particularly via fraud (including bank fraud and stock market manipulation fraud) and identity theft.

The lack of data means that a clear understanding of the scope of these crimes is not possible. INTERPOL reports that violent commodities, such as killing for hire and the trade of small arms, are facilitated by dark web marketplaces, though those marketplaces are not named (INTERPOL 2018g). Moreover, sophisticated cybertools used to conduct criminal acts are commonly found in every country throughout the region in places where the internet exists.

INTERPOL states that the Southern African region may be “a primary location to launder proceeds of crime on a global scale” (INTERPOL 2018g). No one country appears to be a haven, but the region as a whole, with large cash-based, informal, and low-regulated economies near to financial hubs with limited controls as one crosses an international border, creates an ecosystem that may be easily exploited by criminal entrepreneurs (INTERPOL 2018g). As is the case in Eastern Africa, alternative remittance services facilitate cross-border transactions. In addition, casinos exist in most countries in the region and facilitate financial services that are useful to money launderers.

No comparable reporting by INTERPOL on other emerging economies or low-regulated regions is publicly available.

FATF

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 to combat money laundering; its mandate was expanded in 2001 to include terrorism financing. It currently has 36 member countries; two observer countries that still must comply with the FATF recommendations; several observer organizations (including the IMF and World Bank) that engage in anti-money laundering efforts but are not subject to the mutual evaluation process; and two regional organizations (the European Commission and the Gulf Co-operation Council) that also are not subject to mutual evaluations since they are collective bodies – their individual members are reviewed separately. The FATF produces several types of publications that include recommendations, mutual evaluations, money laundering methods and trends, and reports on corruption. In addition, FATF maintains a list of high-risk and other monitored jurisdictions, which is regularly reviewed. This includes those countries on a ‘grey list’ required to grant more intensive surveillance by FATF’s International Co-operation Review Group (ICRG) because of their greater vulnerability to money laundering – a delicate term that includes those who might embrace laundering. Historically, cyber-laundering has been a very modest component of such vulnerabilities. In 2019, a few countries on the list were associated with cybercriminal events; North Korea, Syria, and Iran all faced indictments by US authorities, while Serbia and Sri Lanka were found to have a high rate of phishing and malicious emails (Symantec 2019).

FATF has briefly considered issues related to cybercrime and virtual currencies and assets in its *Report to the G20 Finance Ministers and Central Bank Governors* (FATF 2018d). The report states that while virtual currencies and assets represent a very small proportion of money transacted in cybercrime, it is a steadily growing phenomenon. Cryptocurrencies have been transacted primarily in fraud and small-scale drug-trafficking cases; however, they are increasingly being used in other cybercrimes. The report says that FATF is actively monitoring the risks associated points of transaction of cryptocurrencies such as pre-paid cards linked to cryptocurrencies, Bitcoin ATMs, and Initial Coin Offerings (ICOs). FATF notes that given the difference in regulatory frameworks vis-à-vis cryptocurrencies, there is a strong likelihood that cybercriminals will find ways to place their money in jurisdictions that have laxer rules. Nonetheless, in October 2018 the Financial Action Task Force (FATF) 'recommended that "virtual asset service providers," which include a broad range of cryptocurrency businesses' be subjected to AML legislation (Moiseienko and Kraft 2018, x).

FATF-style Regional Bodies

There are nine FATF-Style Regional Bodies:

- Asia/Pacific Group on Money Laundering (APG) based in Sydney, Australia;
- Caribbean Financial Action Task Force (CFATF) based in Port of Spain, Trinidad and Tobago;
- Eurasian Group (EAG) based in Moscow, Russia;
- Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG) based in Dar es Salaam, Tanzania;
- Central Africa Anti-Money Laundering Group (GABAC) based in Libreville, Gabon;
- Latin America Anti-Money Laundering Group (GAFILAT) based in Buenos Aires, Argentina;
- West Africa Money Laundering Group (GIABA) based in Dakar, Senegal;
- Middle East and North Africa Financial Action Task Force (MENAFATF) based in Manama, Bahrain;
- Council of Europe Anti-Money Laundering Group (MONEYVAL) based in Strasbourg, France (Council of Europe).

These bodies produce mutual evaluations of their member countries and provide technical assistance and training. The relevant reports are reviewed with the countries considered in this research. A fair current summary is that cryptocurrency laundering is widely perceived as an emerging problem, but evidence is sparse and there are many forms of laundering – such as trade-based money laundering - that are also hard to counteract. The proportion of cybercrime that such laundering accounts for is not well understood.

Summary of the State of Play

In evaluating countries with significant internet populations and international regulatory bodies and law enforcement organizations that operate with an administrative language of English, we have noted the following four trends: technological development; geographical offending patterns; law-enforcement capacity and regulation; and investigative objectives.

First, the countries surveyed fall into two groups based on their economies and their technological development: developed countries (Australia, Canada, the United Kingdom, the United States) and emerging countries (India, Nigeria, South Africa). Generally speaking, this divide illustrates significant differences in economic and technological capacity. While developed countries vary in terms of the resources available and strategies in place to respond to cybercrime and cyberthreats, they are far more likely to have the internal capacity to cope with cybercriminal activity than emerging countries. Developed countries have developed governmental and non-governmental resources, including education, investigative units, and legislation, that consider the responses that cyber-based threats require. Moreover, developed countries are more likely to produce publicly available reports that provide insight to the depth and breadth of the cyberthreats the countries are facing.

By comparison, emerging countries do not have developed cybersecurity capacity. Emerging economies face several challenges. It appears that many lack domestic education institutions capable of training people to respond to cybercrime and to develop endogenous cybersecurity systems. Notably, these countries engage in technological leapfrogging in various aspects of ICT; however, despite quickly improved ICT infrastructure, many of these countries lack government- or private-administered capacity to respond to cybercrime and prepare for cyberthreats. If emerging countries produce reports, they are either not available for public consumption or appear to be somewhat superficial. These deficiencies make it difficult to develop an accurate snapshot of the extent to which cybercrime and cybercriminals are present in these countries.

Second, crimes tend to be associated with geography, with technological capacity in the countries from which offenders operate determining the most common crimes committed. The literature indicates that cybercrime actors operate from places which offer the opportunity to develop their knowledge and to access reasonably reliable ICT infrastructure. Accordingly, countries like the US and the UK have a reasonably large share of technically able potential offenders. The same is true, based on law enforcement estimates, for eastern European countries and Russia. However, though their diasporas are less restricted, countries with relatively poor ICT infrastructure and education, such as Nigeria, rely on lower-technology crimes, including business email compromise, 419 scams, romance fraud, and the recruitment and running of money mules, often through fraudulent or manipulative means that can be conducted at internet cafes (Adomi and Igun 2008), though the latter reference is now old in cyber terms.

Third, most countries appear to be in the process of developing legislation and law-enforcement capacity to respond to cybercrimes (The Law Library of Congress 2018), though many cybercrimes are charged and prosecuted using existing non-cyber-related statutes. Likewise, most countries are developing regulations to respond to the emerging, digitally-based payment systems – most notably cryptocurrencies – that the internet affords, again defining these new assets within existing regulatory regimes. Though cryptocurrency presently represents a small proportion of all proceeds of crime, that proportion is increasing. Per FATF guidance, many countries are adopting regulatory standards to oversee a variety of cryptocurrency-related businesses, such as wallets and exchanges, in an effort to prevent (or at least reduce) money laundering and terror finance. Licencing is uneven, with compliance varying greatly, depending on jurisdiction and process type (e.g. licensing and KYC checks) (Hileman and Rauchs 2017). If regulation improves in some jurisdictions, it is likely that some cyberoffenders will gravitate physically or electronically to countries or products with weaker regulatory standards (Moiseienko and Kraft 2018), at least if it fits their cultural and other preferences.

A notable difference, however, between developed and emerging countries is vis-à-vis virtual assets, such as cryptocurrency. Developed countries appear to favour regulation, rather than restriction or prohibition. Developing countries do not follow a consistent trend, with some enacting FATF recommendations, others enacting little or no regulation, and others enacting outright bans of cryptocurrency. Sometimes, the rationale of bans has to do with maintaining control over monetary policy (e.g. India), though this is not universally the case (The Law Library of Congress 2018).

Fourth, regardless of capacity, there appears to be a focus on the big picture of cybercrime, with countries and private enterprises looking to curb illicit activity via *prevent* and *protect* strategies. While there is some capacity being developed for *prepare* strategies by establishing organizational methods to respond to cybercrimes, the capacity to engage in *pursue* strategies is concentrated on “big busts” and often fails to help individuals who fall victim (R.J. Anderson, Shumailov, et al. 2019) even though technological capacity has improved and recovery costs have slightly decreased over time (Ponemon Institute 2019). Some researchers have identified pursue strategies for virtual currencies (R.J. Anderson, Shumailov, et al. 2019; Bistarelli, Mercanti, and Santini 2018; Bistarelli, Parroccini, and Santini 2018; McGinn et al. 2016), but the extent to which these forensic operations have been adopted by law enforcement is unclear and are likely restricted to law enforcement operations in developed countries with higher IT capacity.

Financial Ecosystems and Currency Properties

In reviewing the transactions related to cybercrimes, we found it necessary to understand the variety of financial ecosystems. We identify six distinct but partially overlapping ecosystems (see Figure 1 for a graphical approximation): fiat currency, assets, digital currency, sanctioned alternative payment systems, unsanctioned alternative payment systems, and bartering systems.

Fiat Currency

Fiat currency is money declared as legal tender that is backed by the government that issues it. The fiat currency system is by far the largest currency system in the world, with a total market capitalization value of more than 90 trillion US dollars (Desjardins 2017). The fiat currency system consists of both physical cash and digital ledgers (e.g. bank accounts or PayPal accounts).

Cash Fiat Currencies

Only 8% of fiat currency is in physical cash (Desjardins 2017), though many developing countries still have robust cash economies (Bech et al. 2018; Arango-Arango et al. 2018). International remittance systems, like Western Union or MoneyGram, serve the recipient party in cash, and are commonly used throughout the world. There are significant alternative remittance systems that operate outside government regulation and banking systems to facilitate person-to-person international transfers. These systems still use predominantly cash paid to brokers who, through various types of arrangements, transfer money from one person to another across borders at a low cost. Systems that function in this way are called, depending on context, *hawala*, *hundi*, *fei ch 'ien*, *chit system*, *poey kuan,* and the black market peso exchange (Shehu 2004; Jost and Sandhu 2003; Richet 2013).

Fiat currencies are likely to be increasingly used in their digital form compared to their cash form, as cashless transactions have been steadily increasing in the 2010s worldwide (Marria 2018; Arango-Arango et al. 2018). Fiat currency is the most commonly targeted currency in both offline crime and cybercrime, due to its large market cap and the relative ease of disposing it. Common crimes that capture fiat currency, using ICT facilitators, include *inter alia*, various types of fraud, and theft.

Digital Fiat Currencies

Digital fiat currencies are fiat currencies that are held in digital rather than physical form. In terms of value, there is no difference between a physical and digital specimen of the same currency. Fiat currencies can be easily transacted digitally among individuals, organizations, banking institutions, and countries. Currently, most fiat currency is held within digital ledgers; there is more fiat currency allocated to holders than physical cash in existence (Desjardins 2017). Payments with digital fiat currencies cost little, are broadly accepted, and are comparatively fast.

Transaction systems exist that serve the digital banking ecosystem, have both domestic and international iterations and include both payment systems and money transfer systems. Payment systems include commonly held debit, credit, prepaid, e-purse (contactless smartcard), automated teller machine (ATM), and point-of-service (POS) cards operated by companies such as American Express, China UnionPay, Discover Financial Services, Japan Credit Bureau, MasterCard Worldwide, and Visa International. These card payments may take place in person, online, or via a mobile device (e.g. mobile credit card) and are often facilitated by payment processing companies that process card payments and sometimes facilitate other user-to-user payments. Notable payment processing companies include PayPal, PagSeguro, Vantiv, Worldpay, and payment processing arms of large banks such as Barclays, Bank of America, and Wells Fargo. These payment systems can cope with a high volume of requests almost instantaneously, are available nearly globally, and operate at a low cost (Bott and Milkau 2016).

Notable examples of domestic banking transaction systems include the automated clearing house (ACH) system in the United States, the Single Euro Payments Area (SEPA) credit transfer scheme in the Eurozone (where it appears the UK will remain party, regardless of the outcome of Brexit), the China National Advanced Payment System (CNAPS) in China, and Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT) and Real Time Gross Settlement (RTGS), all in India.

Entities that wish to transfer money internationally may do so by initiating a transfer from their bank or by using a service such as XE.com Inc. or Transferwise, which may, ultimately, use hawala principles in terms of balancing their internal ledgers rather than actually transferring their customers' money across borders. The most used international banking transfer system is the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Notably, China uses its China International Payments System (CIPS), a service that some Russian banks also use. In addition, Russia is developing its own system, SPFS (derived from the transliteration of the Cyrillic acronym, Спфс: Система передачи финансовых сообщений), ostensibly as an alternative to SWIFT to allow it to continue to engage in international transactions even if it is under sanctions that preclude its capacity to use the SWIFT system.

Most digital fiat transfers are traceable; however, there are exceptions. Users can pay with prepaid payment cards or gift certificates, thus concealing their identity (Hernandez et al. 2018). Additionally, some money transfer agencies do not require identification, fail to identify counterfeit identification, or through corruption turn a blind eye to criminal actors, allowing recipients to remain anonymous[4] (Whitty and Ng 2017; Wilhoit and Hilt 2015).

Historically, banking payment systems have been targets for cybercriminals. There existed a high prevalence of payment fraud via the ACH system and there have been notable thefts via the SWIFT system, notably the Bangladesh Bank heist in 2016, and the SPFS system in Russia (Federal Reserve Board 2018; Moiseienko and Kraft 2018; SWIFT 2019). However, recent improvements to both the ACH system and SWIFT system, in terms of identifying fraudulent and unauthorised transactions, have significantly reduced the amount of funds stolen via these systems (SWIFT 2019; Federal Reserve Board 2018). Nonetheless, digital transactions figure heavily in cybercriminal activity, particularly as cybercriminals develop strategies to develop fraudulent accounts or to use money mules and to monetise stolen information such as payment card information.

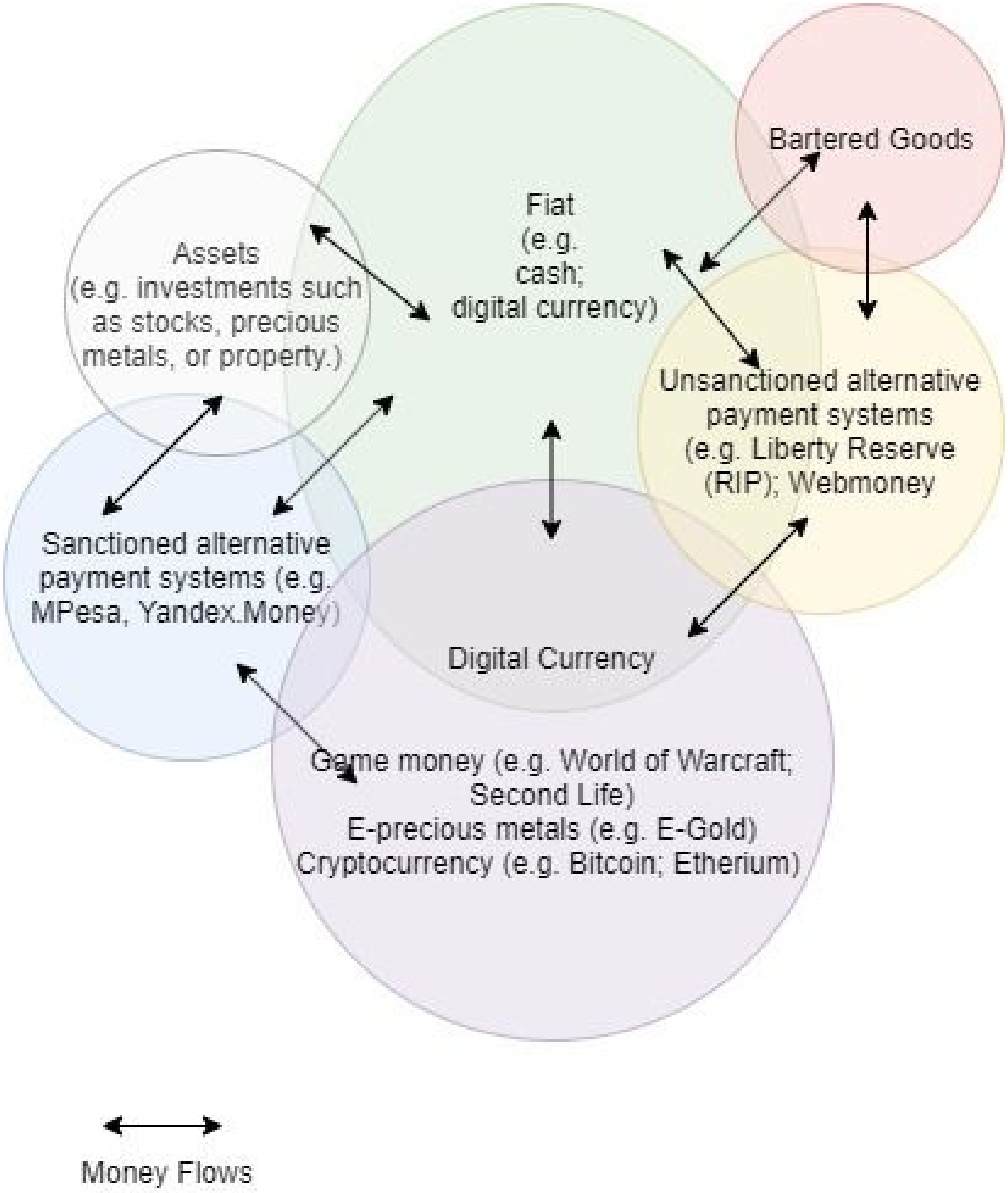

Figure 1: Financial Ecosystems

Assets

Assets are possessable items that hold value, such as real estate and precious metals, and non-currency instruments such as stocks, bonds, and debt (Desjardins 2017). Most of the wealth in the world is held in offline assets. Assets can be purchased using fiat, can be bartered, and, in limited instances, can be purchased using non-fiat currencies. Large-scale purchases of assets using non-fiat currencies remain unusual.

The cybercrime literature does not focus on the theft or use of offline assets at all within cybercriminal ecosystems. It appears that cybercriminals seldom attempt to use the non-fiat proceeds of their crimes to purchase assets directly; instead, they convert their non-fiat proceeds to fiat currency first. Our review has not uncovered the targeting of traditional assets in cybercriminal activity.

Non-Fiat Digital Currency

Outside of digital fiat currencies, digital currency includes digital currencies in videogaming ecosystems; and virtual currencies, which are also commonly referred to as cryptocurrencies. We identify two principal subsystems here: digital currencies and assets in videogaming ecosystems and virtual currencies/cryptocurrencies.

Digital Currencies (and Assets) in Videogaming Ecosystems

There are several virtual currencies within video gaming ecosystems used to buy virtual assets within those games (Gainsbury and Blaszczynski 2017). Early examples include the Linden Dollar used in Lindon Lab’s online virtual world *Second Life,* and WoW Tokens used in Blizzard Entertainment’s massive, multiplayer online role-playing game (MMORPG) *World of Warcraft* (Glaser et al. 2014). Contemporary examples include V-bucks used in Epic Games’ online video game *Fortnite* and Revelation Online Imperial Coins used in NetEase’s *Revelation Online*. Various marketplaces facilitate the trading of these currencies, along with digital assets associated with videogames, such as skins, in-game items, and keys to unlock in-game items for similar items or fiat currency. There are no estimates of the market capitalization of digital currencies and assets in gaming ecosystems. There is some evidence of cybercriminals targeting gaming ecosystems to generate funds by selling stolen digital assets, to cash out proceeds of crime, or to launder money (Moiseienko and Izenman 2019; Gault 2019). However, without market cap figures, estimating the current or potential volume of this laundering is not possible.

Virtual Currencies/Cryptocurrencies

By definition, “a virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community” (European Central Bank 2012). Cryptocurrencies form a subset of virtual currency that uses distributed ledger technology – often a blockchain, which involves a growing list of records, called blocks, that are linked using cryptography – to record transactions and manage the issuance of new units of that currency (Egan 2018). The use of cryptography attempts to prevent counterfeiting and fraudulent transactions. Non-state-sponsored virtual currencies are not legal tender, meaning that they cannot be used for settling private liabilities, tax, and other government payments; nor can they accrue interest (Bott and Milkau 2016). Unlike regulated electronic money schemes, which offer an escalations process that customers can use to file a claim in the event of a dispute regarding a transaction, within cryptocurrency payment ecosystems, transactions are irrevocable (Samani, Paget, and Hart 2013). Moreover, when vendors accept cryptocurrencies, they generally peg prices to fiat currency using exchange rates (Bott and Milkau 2016).

Cryptocurrencies usually are decentralised, without any central issuing or regulating authority (Brito 2014), but a few central-bank issued cryptocurrencies have been mooted and are in various stages of development in China, The Eastern Caribbean Currency Union, Estonia, Iran, the Marshall Islands, Russia, Sweden, Tunisia, Turkey, and Venezuela (Mahdavieh 2019; Shanaev et al. 2020; Blakstad and Allen 2018). More recently was the proposal of Libra, a cryptocurrency in development by Facebook and the Libra Association as a universal payment system (Libra Association Members 2019). Libra’s future, however, remains uncertain as nearly all payment companies that had initially supported Libra’s development have withdrawn their support (Paul 2019).

Cryptocurrencies can be legally obtained by mining them, charging transaction fees, purchasing them with fiat currency or other cryptocurrencies, or accepting them as payment for goods or services (Egan 2018). Successful mining operations solve a cryptographic puzzle determined by an algorithm. Transaction fees help to incentivise miners to continue when the difficulty to successfully solve a problem increases and becomes more resource intensive and less profitable to continue mining. The purchase of cryptocurrency can happen at an exchange, via peer-to-peer networks, via a deduction in phone credit, and in some limited applications with cash at a payphone, broker, or a specialised ATM (Sirila 2014). Not all options are available for all cryptocurrencies as support varies considerably, with most cryptocurrencies having extremely limited support and acceptance (Elendner et al. 2018; Hileman and Rauchs 2017).

Bitcoin, established in 2009, was the first widely successful cryptocurrency, and remains the most used. Bitcoin is pseudo-anonymous, meaning that the transactions can be traced from account to account, but the account holders cannot be known unless further information associated with the account holder is able to be revealed. True, on-the-chain Bitcoin transactions have become increasingly more expensive and are slow, taking minutes (Girasa 2018; Bratspies 2018); by comparison, transactions with a payment card are consistently cheap and quick. To resolve this problem, exchanges often engage in off-the-chain transactions, where they credit digital ledgers with transaction value without processing the payment through the blockchain until a customer wishes to withdraw funds (Poon and Dryja 2016).

At the time of writing, coinmarketcap.com, a website that monitors cryptocurrencies, their values, and the markets that trade them estimated that there are 3,047 distinct cryptocurrencies; 20,897 markets that trade in cryptocurrencies; a total market cap of $252,078,760,945, with 67.5% of that value comprised of Bitcoin ("Coinmarketcap: Cryptocurrency Market Capitalizations" 2019). To put that number in perspective, the overall market capitalization of cryptocurrencies is 0.00000679347 of the world’s easily accessible money supply ($36.8 trillion in 2017) (Desjardins 2017). Following Bitcoin (1, in terms of market capitalization) is (2) Ethereum (ETH), (3) Ripple (XRP), (4) Bitcoin Cash, and (5) Tether. Other popular cryptocurrencies mentioned in the literature include (6) Litecoin (LTC), (7) Binance Coin, (13) Monero (XMR), (19) Dash, and (30) Zcash ("Coinmarketcap: Cryptocurrency Market Capitalizations" 2019), some of which proport to solve some of the deficiencies of Bitcoin’s cost, speed of transaction, and privacy (Girasa 2018).

The overall market capitalization, presence of cryptocurrencies, and presence of markets are extremely volatile. The usage rate of cryptocurrencies as a proportion of everyday expenses is also limited with comparatively few vendors accepting a small number (usually only Bitcoin) cryptocurrencies for purchases. Again, cryptocurrency acceptance is volatile, with some licit vendors ending acceptance in the wake of regulation, difficulties in establishing or maintaining payment processors who pay out vendors in fiat currency, or – as is particularly the case with Bitcoin – increased transactional fees that make smaller payments less viable (Hileman and Rauchs 2017; Kim 2019). Until cryptocurrency transactions become widespread, it is unlikely that the volatility in their markets will stabilise. The extent to which a cryptocurrency is likely to become widespread hinges on its capacity to have usability, security, acceptance, reliability, and volume[5] (Dion-Schwarz, Manheim, and Johnston 2019). Ultimately, it appears that most cryptocurrency users invest in cryptocurrencies as speculative investments, with a hope that the value appreciates (Selmi, Tiwari, and Hammoudeh 2018; Don, Clarke, and Jiang 2019) rather than making an attempt to switch to an unregulated alternative currency, as was the starting ethos of Bitcoin.

In terms of cybercrime, cryptocurrency, as a significant element, is typically involved in the following crimes: the purchasing of illicit items, such as controlled substances or weapons; extortion, such as requests made via ransomware or to relent a DDoS attack; theft, such as the stealing of cryptocurrency from exchanges or “hot” (online and connected) e-wallets; purchasing precursor items to commit further cybercrimes, such as purchasing how-to guides or cloud bullet-proof hosts to run botnets or ransomware or host child exploitation materials; purchasing crimeware-as-a-service, such as renting pre-produced ransomware; and, cryptojacking, the unauthorised use of another computer’s resources to mine cryptocurrency. The most commonly cited cryptocurrency in cybercriminal applications is Bitcoin (Christin 2017; Cronin 2018; Ghosh et al. 2017). However, given that Bitcoin is pseudo-anonymous, there appears to be an emergence of the use of other, more privacy-focused, coins such as Monero, Zcash, and Dash (Moiseienko and Kraft 2018; Chainalysis 2018; Ducas and Wilner 2017; Girasa 2018).

Sanctioned Alternative Payment Systems

Sanctioned alternative payment systems facilitate payment for goods and services using technologies that transact value outside traditional payment systems, such as cash or payment cards, with the approval and regulation of a government. The most common type is mobile money, also known as branchless banking (Reaves et al. 2017). Mobile money is a payment service that allows a customer to use a mobile phone to pay for a wide range of services and digital or hard goods or transfer money to another user’s account, both inexpensively and quickly. In 2018, there were more than 866 million registered accounts in 90 countries with USD $1.3 billion transacted every day; most of these users are unbanked or underbanked (Pasti 2019). The most common mobile money transactions are putting cash into or removing cash from the system, but digital transactions have grown, driven largely by bill payments and bulk disbursement (Pasti 2019), increasing further adoption of these services in lieu of using cash. There are typically limits to the size of transactions and value held in the accounts (Runde 2015). In addition, governments regulate these systems across five areas: taxation, KYC requirements, cross-border remittances, national financial inclusion strategies, and data protection (Pasti 2019).

The first and most successful of these systems is M-Pesa, a mobile money system launched in 2007 by Vodafone for Safaricom and Vodacom, the largest mobile network operators in Kenya and Tanzania (Reaves et al. 2017; Sirila 2014). M-Pesa has since expanded, with varying degrees of success, to other countries. M-Pesa was inspired by unbanked users who transferred airtime as a proxy for money (Runde 2015). To use the M-Pesa system, users load value onto their accounts using a broker. They can then trade this value as payment. Users can withdraw value from their accounts by using a broker. The system collects small fees on transfers and cashing out.

As noted, there are hundreds of similar mobile money systems around the world. Some, such as Argentina’s Mercado Libre and Jamaica’s M3 Mobile Money for Microfinance, are also providing non-transactional banking services, such as microfinancing (Pasti 2019; Bissessar 2016). Some services, such as Yandex.Money in Russia or Yellow Pepper in several Latin American countries, provide hybrid services that serve as traditional payment card processors as well as mobile money services. While most money services focus on populations in emerging markets, they also impact diaspora populations living abroad that attempt to remit money. In addition, there are ad hoc transferring services present in the developed world, such as Venmo in the United States, Paym in the United Kingdom, Vipps in Norway, and Swish in Sweden.

The emergence of mobile banking does present some concerns. In terms of regulation, there may be limitations in KYC if underserved people have problems obtaining identification. The solution so far appears to be capped accounts that do not require identification, the use of SIM registration data in lieu of ID, or the use of e-KYC (Pasti 2019). To that end, there is a risk of smurfing accounts, that is using several unidentified accounts to launder money, as well as user exposure to fraud facilitated by phishing and other human engineering efforts (Zhdanova et al. 2014; Akomea-Frimpong et al. 2019; Deloitte 2015). Theft are other concerns: there are up to 3,000 cybercrimes a month in Kenya as well as attempts to hack into M-Pesa (McGuire 2018). Given the low incomes of many users in this space, thefts could represent a much higher percent loss; however, if pursuit trends around the world hold, it is our view that it will be unlikely for law enforcement to invest many resources in recovering or investigating these crimes, thus necessitating systems to enact endogenous security measures to reduce these risks.

In addition, Yandex.Money has been commonly accepted in darknet and Clearnet grey marketplaces that sell items, such as bulletproof server space, that could be used to facilitate a cybercrime (Moiseienko and Kraft 2018). Another licit payment method cited in the literature is the use of Ukash (Samani, Paget, and Hart 2013), an online voucher system that was acquired by Skrill and folded into paysafecards. Users can purchase paysafecards which are single use serial numbers and can either pay accepting merchants using those serial numbers or transfer those serial numbers to another user to use. Green Dot MoneyPak is a similar system of prepaid payment cards, that targets a US customer base. Paysafecard serials and MoneyPak prepaid cards have been methods by which ransomers have requested payment, given the cash-like properties of the serial numbers (R. Anderson, Barton, et al. 2019). That these alternative payment systems, operating at the margins of KYC, could facilitate payments for illicit goods is not beyond the realm of possibility.

Unsanctioned Alternative Payment Systems

Unsanctioned alternative payment systems have endured outside any government regulation. As noted above, hawala-type systems have long existed to credit cash to parties in distinct, often international locations. Cryptocurrency, in its inception, was also meant to be an unregulated, non-governmental controlled payment system; regulation has decreased the viability of some cryptocurrencies to function entirely outside government oversight, particularly at the point of cashing out into fiat currency. However, there are some alternative payment systems that have existed and continue to exist outside government oversight.

A few notable payment systems are now defunct, having either closed operations voluntarily or been shut down by law enforcement (White 2014). These early systems included *inter alia*, E-gold, and Liberty Reserve (Samani, Paget, and Hart 2013; White 2014; Mullan 2016). In short, these systems provided unregulated transactional platforms that transferred value between actors, internationally, outside the banking system, without the need to provide verifiable information (Mullan 2016).

E-gold was the first of these systems, established in 1996, and running until its operators were indicted in 2008 (Mullan 2016). Every E-gold account balance, which may be held in any of one of several e-precious metals, including gold, silver, platinum, and palladium, was fully backed “gram for gram, by physical precious metal held offline” in secure vaults (Mullan 2016, 21). At its peak, E-gold was only second to PayPal in the online payment industry, transacting between USD 1.5 and 2 billion in 2005 (White 2014). When US investigators determined that E-gold was being used by sellers of child pornography to accept payment, operators of investment scams, and carders to transfer the proceeds of their crime, since it circumvented currency controls, US federal authorities targeted E-gold for not adhering to licensing standards (Mullan 2016; White 2014; Trautman 2014). (Notably, E-gold, in contrast to other internet payment systems, did not include a statement in its terms and conditions that prohibited its use for criminal activity (Ogunbadewa 2014).) The resulting court case found against E-gold's operators, though it viewed their actions as unintentionally criminal; tens of millions of dollars were held, unable to be released to account holders, when trading was frozen (White 2014).

Replacing E-gold on the mantle of non-attributable transactional systems (such as those that would appeal to cybercriminals) was Liberty Reserve, a company that provided a means to transact outside the banking system with its own currency, the Liberty Reserve Dollar (Mullan 2016). Liberty Reserve ran publicly from 2007 until it was seized in 2013 by the US Treasury Department, the first exercise of the US Patriot Act (Trautman 2014). However, Liberty Reserve began to run into operational obstacles two years earlier when it was not granted a business license in Costa Rica, where it had been incorporated.

Liberty Reserve was user friendly. Users could establish accounts without any legitimate identification and the Liberty Reserve Dollar was easily transacted for fiat currencies by brokers in countries throughout the world (Leukfeldt, Kleemans, and Stol 2017). Additionally, Liberty Reserve funds could be spent via '"No ID" debit cards that furnished instant access to the cash value of Liberty Reserve's digital units' (Mullan 2016). Liberty Reserve made its money by taking a 1% commission on transactions and by charging a fee to erase one's account number from the transaction, thus providing anonymous transactions (Trautman 2014). Like E-gold before it, Liberty Reserve was popular among criminal actors, who used it as a transaction platform that allowed them to circumvent currency controls at a global scale (Trautman 2014; Mullan 2016).

Upon the fall of Liberty Reserve, it appears that many of these "privacy-minded" customers went to PerfectMoney (https://perfectmoney.is/), based in Panama but with its servers in Iceland (Mullan 2016). [6] PerfectMoney is a service that has operated at least since 2013, and which, at the time of writing, is still in operation. PerfectMoney operates several transfer services, including the production of e-vouchers to send to others, even if the recipient does not have a PerfectMoney account. PerfectMoney is still accepted in some darkweb and grey markets as a means of payment and has been used in “high-yield investment programs (HYIPs), online Ponzi schemes where existing investors are paid lucrative returns from the contributions of new investors” (Vasek and Moore 2015, 2). PerfectMoney says it complies with AML standards in Panama, though this claim is not verifiable, and those standards themselves are under ongoing review.[7]

Another platform that the literature commonly cites is WebMoney (https://www.wmtransfer.com/). WebMoney use involves “guarantors” or escrows who underwrite transaction amounts and ensure that funds are smoothly transferred from buyers to sellers and that payments are anonymous (Wilhoit and Hilt 2015). It is possible to make payments to other users without knowing their identity. WebMoney has different levels of verification following KYC standards, and is registered as an “Authorised Electronic Money Institution” with the UK Financial Conduct Authority,[8] though it is required to comply with the requirements in regulation 78A(2)(b)of the Electronic Money Regulations 2011 to refrain from providing account information services or payment initiation services for an indefinite period.

Bartering Systems

Bartering systems exist to trade goods and services in exchange for other goods or services. In cyberspace, they are commonly found in communities that trade in child exploitation material, where the materials are not necessarily traded for monetary gain but to increase the number of images an actor possesses (Beech et al. 2008; Merdian et al. 2013). Some bartering has been observed in Darkweb marketplaces where products or services are offered in exchange for prepaid debit cards, online gift vouchers, such as paysafecards, and prepaid payment cards for music or video games (FTR Team 2015; Urano 2015).

Getting paid in this way protects the anonymity of both buyer and seller and obviates the need to engage in unusual, perhaps unwieldly, payment structures that alternative payment systems may present (Agari Cyber Intelligence Division 2019). Other bartered transactions, such as *quid pro quo* for goods and services, may also occur in the darkweb, though the nature of those transactions tends to be private and is not documented; it is unclear that existing darkweb escrow services hold anything apart from cryptocurrency.

Regulation

Whether payment in a criminal ecosystem is viable depends, in part, on successful regulation. Regulation can be considered a two-part process: first, there is a need to establish appropriate rules to curb unwanted behaviours. Second there is a need to enforce those rules, which entails investigating infractions and punishing rule breakers, whether they be financial intermediaries or what we might term ‘primary offenders’, i.e. those who commit the predicate crimes whose proceeds are being laundered. Sometimes, these categories are fused, as when those who manage cryptocurrencies themselves or exchange websites defraud their customers.

The literature shows that several countries have pushed to regulate developing transactional systems, whether by simple prohibition or by licensing. This move is evidenced by the takedowns of E-gold and Liberty Reserve as well as the increased efforts to regulate cryptocurrency exchanges and other money transferring businesses trading in non-fiat currency (The Law Library of Congress 2018; Kshetri 2017; Sotiropoulou and Guégan 2017; Lycka 2011; Williams 2006; White 2014). It is no more defensible to point to the existence of fraud or money laundering as a ‘regulatory gap’ than it is to assert that every other form of crime reveals a regulatory gap. However, there remains profound uncertainty about the inherent threat of cryptocurrencies to both conventional regulatory bodies (like the Bank of England and US Treasury) and society at large. To the world of banking and regulation, blockchain is one thing; cryptocurrencies are another. One consequence of this distinction with regulatory frameworks is that there exists the possibility of regulatory arbitrage, particularly in nations that lack the capacity or the desire to engage in regulation and its enforcement. Another is questions that arise for the collection and cross-border passage of electronic evidence. The UK has negotiated a treaty with the US, but the EU has yet to do so, let alone all other jurisdictions. Problems with jurisdiction, including the collection of evidence, render enforcement difficult (Kleijssen and Perri 2017).

Second, there is the question of tolerance to low-value crimes. Given the volume of financial transactions, most financial institutions do not investigate “small” losses; instead, they build those losses into their business model. These thresholds are proprietary information. Nonetheless, it is likely that, through trial and error (and perhaps inter-offender risk communication), experienced criminals will develop an understanding of the limitations of individual transfers and operate below those thresholds, perhaps creating “smurfing” operations that use many transactions to turn over large amounts of capital (Zhdanova et al. 2014). Moreover, given that small frauds are unlikely to be investigated by police, who often lack the capacity or judge such cases as cost-ineffective, these margins to commit financial crimes will likely persist at volume unless investigators develop the capacity to connect small-value crimes to a broader set pattern efficiently via criminal network analysis. It is not clear that there are any good role models for doing so, but heavy criticism of police responses both to fraud (HMICFRS 2019b) and to cyber-dependent crime (HMICFRS 2019a), as well as media ‘undercover expose ethnographies’ of Action Fraud in *The Times* indicate that England and Wales offer only modest performance to date.

Third, there is the question of technical capacity to detect regulatory compliance cheaters. In terms of cryptocurrency, prior studies have identified key exchanges – such as the now-defunct BTC-e – that cybercriminals have relied on in order to transact the proceeds of their crimes (R.J. Anderson, Shumailov, et al. 2019). These activities do not appear to be ongoing. Yet, identifying exchanges or other spaces where cybercriminals transact their funds can help identify bottlenecks that can be more easily sealed or loopholes in regulation that innovative cybercriminals learn to exploit. Moreover, many developing countries lack endogenous education systems capable of training people with adequate cybersecurity skills and the capacity to investigate these crimes (Oleksiewicz 2019), though the Council of Europe and UNODC have active programmes of development.

Constructs of ‘economic crime’ vary (Levi 2015), but what is clear is that there are no equivalent evaluations for cyber-enabled crimes similar to the formal country evaluations of money laundering or of corruption that are routinely produced,[9] and FATF-style evaluations have cyber-laundering as only a modest part of their profile. Not all cryptocurrencies run on permission-less, public networks. Ripple requires users to be validated before they engage in any sort of transaction on its network, but, unsurprisingly, FATF has suggested that governments should delegate powers to monitor and assess users and transactions to central authorities, rather than to self-regulatory bodies such as Ripple. There is an ongoing dialogue with the private sector, which in 2019 has already led the FATF to modify its 2018 position:[10] although FATF has strong Treasury representation, it seems unlikely that a globally uniform model will be developed and accepted. FATF may feel constrained not to increase its cyber scrutiny in the current round of evaluations because of its need to be consistent with past evaluations. As a result, despite the relative non-invasiveness of FATF’s evaluations, it may take years for cryptocurrency issues to be fully integrated into FATF’s Mutual Evaluation Reports, though FATF and the International Financial Institutions, such as the World Bank, could encourage National Risk Assessments to look at this set of issues.

Criminal Ecosystems (Actors, Products, and Crime Scripts)

In considering the various types of cybercrime – cyber assisted, cyber enabled, and cyber dependent – we turn to evaluating criminal ecosystems to help establish the parameters that influence how transactions associated with aspects of the preparation and/or commission of these crimes are likely to unfold. In considering these criminal ecosystems, it is important to note that, like offline offending, many jobs and tasks are compartmentalised and undertaken by specialists (Broadhurst et al. 2014; Bayoumy 2018).

In considering criminal ecosystems, we outline the products involved and propose outline scripts of the crime as examples of how they may unfold. Crime script analysis details the sequential steps required to carry out a criminal event. For cyber-dependent crimes, crime script analysis involves detailing the process whereby cyberoffenders commit their crimes, offering an opportunity to identify the various points where cyberoffenders monetise their crimes throughout the criminal event. In this section, we rely on findings from the literature review to detail the crime scripts of cyberdependent crimes.

Unfortunately, our review of the literature identified few studies that had access to primary data on cybercrimes, with even fewer having access to primary data on cybercrimes as it relates to financial ecosystems. This lack of data means that visualizations of these crimes are not possible to produce or risk being misleading, being based on iconic investigated cases. From the review, a total of 42 articles were coded as having information that detailed the crime commission process. These articles varied in the types of cyberoffences committed (e.g., attacks against point of sale systems, botnets, sale of illicit products on online markets, phishing), as well as the level of detail on the crime commission process – with most providing information on isolated stages rather than the full set of stages to carry out the crime. Accordingly, we offer outline crime scripts, developed by evaluating products observed for sale by darknet vendors and actions discussed within the literature. We offer one advanced crime script analysis of botnet attacks, which was the most consistently detailed across the various articles and reports.

However, the crime script analysis should be interpreted within the limitations of the data. Importantly, the crime script analysis relies on secondary data from a literature review. Because of this we do not know the full details of the criminal event. Many articles and reports did not disclose how data was collected, and there was no systematic framework across the studies detailing the crime commission process.

While multiple articles detailed various segments of the crime commission process, there rarely connected the series of events across these different segments. Crime script analysis requires systematically coding the crime commission process from the onset of the crime until its end. Future research support should fund studies that engage with heretofore untapped primary data sources, such as what might be collected in “digital ethnographies,” in order to detail the full crime commission process from the beginning of the cyberoffence until its completion (Brewer et al. 2019). These studies may draw from the crime script literature, which has relied on various data sources to map out the scripts of various crimes. These data sources include i) digital trace data, ii) official sources, and iii) self-reports. We outline each data type and describe how it may further our understanding of cyber-assisted and cyber-dependent crimes below.

Digital trace data consists of online material made available and archived via online platforms. For crime script analysis, this has primarily involved discussion forum data. For instance, in a study detailing the online stolen data market, Hutchings and Holt (2015) relied on 13 web forums where buyers and sellers came together to purchase and sell personal data. A content analysis of the nearly 2,000 exchanges between buyers and sellers detailed descriptions of how the stolen data was acquired, advertised by the sellers, how payments were made, and how currency was laundered (Hutchings and Holt 2015). Together, this provided important insight into the operations of online stolen data markets.

Official sources, in particular law enforcement investigative data, collate detailed information about the crime commission process. Seized hard drives, wiretaps, and interviews with officers and prosecutors involved in the investigation of the cyberoffence have all been used to reconstruct the commission of cybercrimes (Dupont 2016; Leukfeldt 2014). Importantly, this information has also been used to reconstruct the relational events – that is how various cyberoffenders converge in time and space in order to carry out the criminal event. This data can then be used in conjunction with network analytic techniques, which are uniquely suited to map out the complex interconnected structure of cybercrime operations. For instance, Dupont (2016) relied on the seized hard drives of cyberoffenders to map out their communication networks and understand how offenders worked together, and Leukfeldt (2014) relied on investigations data in order to understand the settings in which cyberoffenders met (e.g., online versus offline environments).

Court records also represent a valuable resource for mapping out crime scripts. In order to secure convictions, court records, such as trial transcripts and sentencing reports, provide a rich source of data containing detailed information on the key players, their connections, and how they carried out the crime. Future studies may systematically review cybercrime court cases in order to understand the modus operandi of offences. Importantly, this data is typically publicly available – one of the main limits of law enforcement records which may not be shared with outside parties.

Lastly, self-report information including surveys and interviews with offenders represent an underutilised data source in cybercrime research. The cybercrime literature is ripe for opportunity for this type of analysis, which few have seized on. The anonymity of online environments and messaging apps provide an important source for directly interacting with offenders and learning about the sequential steps required for carrying out a criminal event. Previous studies have emphasized the utility of surveys for reconstructing crime scripts (see, for example: Beauregard et al. 2007). Together these sources provide detailed information which outlines the sequential steps required for carrying out a criminal event, providing a promising framework to identify the various monetization processes and how offenders cash out from cyberdependent crimes.

Criminal Marketplaces, Darknet Vendors, and Grey Deepweb Vendors

Criminal marketplaces that sell illicit consumable products and services exist in several contexts. The most common marketplaces appear to be in English and Russian, though other marketplaces in Chinese, German, French, Spanish, and Japanese have all been identified (Gu 2014; Trend Micro 2016a; Ciancaglini et al. 2013; Urano 2015; FTR Team 2015; Wilhoit and Hilt 2015; Pernet 2016; Trend Micro 2016b; Goncharov 2015). It appears that in these marketplaces, some products are tailored for use or exploitation in specific markets; other products appear more generally and are available for capable users to exploit them as they see fit (Check Point 2019; Samtani et al. 2018). Accordingly, we have compiled a list of some products in attempt to identify likely products that can be exploited for cybercriminal ends. These products provide a plausible baseline to estimate costs of some common attacks.

General availability of tools and advertised costs

- **Ransomware, Exploit Kits, and Malware.** The sale of ransomware, exploit kits, and malware is well catalogued in the literature (Bayoumy 2018; Salvi and Kerkar 2016; Cusack and Ward 2018; Etaher, Weir, and Alazab 2015; Chu, Holt, and Ahn 2012; Sigler 2018), with software of varying degrees of customization and sophistication available. We believe that low price points reported, ranging from 2 to a few hundred dollars, are consistent with the advertised selling points for items we found advertised, but we are unable to confirm the efficacy of the products sold[11].

- **Distributed Denial of Service (DDoS).** DDoS attacks are used to disrupt services (Manky 2013). They are sold as a service. We did not find many options; the one we did charged $600.[12]
- **Data.** As noted in the literature, *fullz*, identity packages that include a data set that is sufficient to reconstruct a person's full identity (Wilk 2017; Broséus et al. 2017) – including their social security number, full name, date of birth, email, city and state of residence, and, potentially, passwords associated with their accounts, are easily and cheaply found. While the existing literature quotes prices of about $5 USD, our research indicates that likely prices could be as low as $1-$2,[13] with the price differential hinging on the date of birth of the victim with a premium paid for DoB's from 1970 onward. This information is useful for fraudsters because it allows the person who poses it to create accounts that can later be used to transact without the individual whose data was stolen being aware. Such accounts can be used as digital cutouts, establishing dead ends for investigations or facilitating accounts in muling and money laundering processes (Broadhurst et al. 2014). Other data is also available such as credit cards, passwords, email lists and other compiled information that can be monetised (Van Wegberg et al. 2018).
- **(Bulletproof) hosting / Remote Desktop Protocol (RDP).** Hosting services are critical for several types of cybercrime, such as command and control structures for ransomware and botnets (Ianelli and Hackworth 2005; Dittrich 2012; Antonakakis et al. 2017; Bayoumy 2018; Cárdenas et al. 2009). In addition, both hosting and RDP can be used to set up a server, which, in turn, can also be used to obscure one's actual location, or to appear to be operating from another location, by routing communications through a remote computer.

Hosting is often just remote access to a shell account, an account that allows a user to run command line operations. Using the command line, a user can configure services such as http, email, Jabber, nodes for darknet websites, etc. This is usually done using Secure Shell (SSH) – a protocol that provides secure remote access to a shell account – to execute commands remotely. Setting up one's own server requires a degree of technical expertise characterised by the ability to configure operating systems and to install services. Rouge hosting services – also known as bulletproof hosts – that specifically advertise a refusal to cooperate with law enforcement, is available (Bayoumy 2018; Cárdenas et al. 2009), as well as grey-market services which are ambiguous in their willingness to cooperate with law enforcement and more open to standard forms of payment such as PayPal and debit and credit cards.

Using RDP requires less technical skill. By comparison, a person using RDP logs into a remote computer and then can run and interact with applications on that computer as if s/he were sitting in front of it. An RDP user can use Windows applications as normal. We found what advertised access to these resources from $1-$30 per month.[14]

- **SOCKS.** Another tool that can be used to obscure one's actual location, or to appear to be operating from another location is SOCKS. SOCKS is an old, simple protocol that allows network packets to be routed through an intermediate computer. We found SOCKS access advertised from between $2-$20 monthly.[15]
- **Virtual Private Network (VPN).** Virtual Private Networks can help obscure activity over a monitored connection. However, legitimate VPN providers are likely to cooperate with law enforcement, so further anonymization is likely to be necessary. However, what is for sale is credentials to legitimate services, which allows one to use the VPN service without ever association one's real identity with an account. A VPN may be used as a part of a chain of obscuring activities such as first connecting through a VPN and then accessing a remote machine via remote desktop (RDP) or SSH - secure shell. VPN credentials are advertised to sell for between $2-$6.[16]
- **Internet Access.** Evidently, stable access to broadband internet access is needed for many technologically dependent cybercrimes. These prices vary widely depending on where they are acquired.
- **Communication Protocols**. There are various communication protocols that one can use and that are free, including Internet Relay Chat (IRC) and Jabber (XMPP) (Smirnova and Holt 2017). To best obscure one's communication, one would want to pipe communications and connections through a lot of different servers, to make it harder to trace. Alternative communication platforms that have had documented use are invite-only, private forums (P. Shakarian and Shakarian 2016; Gautam, Gahlot, and Kamat 2019; J. Shakarian, Gunn, and Shakarian 2016; Ablon, Libicki, and Golay 2014) and Telegram, an encrypted communication platform (Check Point 2019). Further encryption methods include using Tails, a live operating system that attempts to prevent unauthorised access from intruders, and OpenPGP, an email encryption protocol (Cusack and Ward 2018).

Botnet Deployment

Botnet attacks represent one of the most serious cyberoffences. Botnets typically refer to an interconnected network of machines (i.e., the 'bots') infected by malware that are simultaneously controlled by a single attacking party (i.e., the ‘botmasters’). Botnet attacks support numerous other online crimes, including Distributed Denial of Service (DDOS), the distribution of malware, and bank fraud. Our analysis of the crime script of Botnets indicated that attacks can follow multiple different pathways from the time a botnet master acquires the botnet to the final exploitation of extracted data and its monetization. In this analysis we focus on the five main steps a botnet attacking group can take in order to successfully carry out an attack, detailing the various points at which attackers’ pathways may converge. Thus, the crime script for botnet attacks is not prescriptive, but rather highlights one common pathway used by attackers, along with how offenders may improvise along the way.

Figure 2 outlines the crime script of a botnet attack. The first step of a botnet attack involves acquiring the necessary technical infrastructure and software to deploy the attack. This step typically requires that the attacker acquire malware that permits covert bidirectional communications. The botnet master must be able to send messages from their server(s) to the infected computer in order to deploy the attack, as well as receive messages from the infected computer back to their server(s) (e.g., whether that be folders, emails, or password to bank accounts, etc) without being detected. The botnet master may acquire the necessary malware to deploy the attack through their own technical competency and programming skills, or they may contract this step out to others. For instance, a botnet master may purchase the malware either through offline channels, or online markets and forums. Botnet masters may acquire malware that has already been developed or reach out to an individual who provides crimeware-as-a-service and have them develop malware suited to their needs. In the latter scenario, the botnet master contracts out the development of the malware, detailing the type of target they wish to attack, as well the type of data they wish to extract.

After acquiring the necessary malware, the second step of a botnet attack typically involves injecting the malware into the highest possible number of targeted machines. The most common method of distributing malware to infected systems are through i) phishing campaigns, and ii) compromised websites. Phishing campaigns typically involve mass emails with compromised attachments and/or spam sent to mobile phones. At this stage, the botnet or compromised mail server may send out spam emails en masse. The malware may be designed in such a way that it is activated once an individual opens an attachment or clicks on an infected link within the email. Alternatively, machines may be infected through spam sent to mobile phones. Attackers have used various means to send spam out to mobile phones, including GSM modems and SMS servers. GSM modems can support multiple SIM cards and can directly connect to a mobile network, allowing them to both send and received text messages. For instance, in one report, it was found that GSM modems can send nearly 10,000 text messages in the span of one hour (Gu, 2014). SMS servers can also be used to send out phishing scams, by sending out a signal that causes mobile phones in the vicinity to disconnect from their network carriers and connect to the SMS server instead. By hijacking the network carriers signal, the spammer may then text out to the phishing campaign numbers. After the SMS server disconnects, the mobile phones are reconnected to their network servers.

In other cases, individuals may create compromised websites in order to distribute the malware. Attackers may hack into websites or may rely on manual low-tech skills. For instance, in one case, attackers purchased a list of passwords and credentials for multiple websites. They then logged into each website, and injected a backdoor, which allowed the attackers to execute commands to access the machines. Similar to the first step, botnet attackers may also elect to contract this step out. For instance, botnet masters may rely on intermediaries to inject the malware into machines. These intermediaries are typically paid on a pay-per-infection rate, where their total payment is proportional to the total volume of machines they infect.

The third step of a botnet attacks involves taking control of the infected machine and integrating it into the botnet’s infrastructure. Because of the scale of botnet attacks, often aiming to attack thousands if not millions of machines, botnet attacks typically transmit communications via servers dedicated for these tasks, which are typically known as command and control servers. These servers aim to transmit commands to the infected machines and in turn receive the relevant data from the infected machines without being detected by either the target or the Internet Service Provider. To avoid detection, botnet masters may employ various protection mechanisms. For instance, attackers may rely on Traffic Distribution Services, which route web traffic with the goal of evading security detection devices. Taking control and exploiting the data of infected machines may take different forms depending on the malware used and the goal of the botmaster. For instance, once the machine is infected, exploitation may begin immediately, or it may require some form of execution by the end-user. For instance, in one case, individuals sent out a word attachment to emails that had a macro function. When the macro was opened, the code was then downloaded to the machine which encrypted all the files and then moved them all into a password provided folder, before requesting payment (i.e., in this case Bitcoin) from the victim in exchange for the password. An example of taking control of the individual's personal folders, and payment system.

The fourth step of a botnet attack involves exploiting the infected machines. This step can take on nearly unlimited forms. Botnet masters may take control over numerous computers to create a DDOS attack, they may inject ransomware, click-fraud, and keylogging software. Additionally, individuals in charge of these operations may elect to rent out their malware to others for their own financial monetization. For instance, one botnet attack involved a large-scale phishing scam. In this scam, individuals that were infected were provided with a toll-free number which instructed callers to call in to receive support for the infection. After calling the toll-free number, the user was put in touch with a technician, who instructed the user to download a remote desktop software, providing them with full control over their machine. From this point, the technician may attempt to demonstrate there are issues on the target's computer and request a fee which may be paid by credit card. The offender can then receive payment, or they may capitalise on their remote access to the computer to extract other personal data.

In the final step, the botnet master may then monetise the exploitation. Depending on the nature of exploitation this may take on various forms. If the goal is to extract personal data, this data may then be sold on cryptomarkets over online platforms such as the Clearnet, Darknet, I2P, or Freenet. Markets on the darknet often use anonymous web currencies. Alternatively, the botnet master may use the personal data for their own gain, such as accessing personal bank accounts through credentials or password protected information. If the botnet attack involves infecting the machines with ransomware, the monetization may involve the payment from the victim. Because victims may be less likely to have cryptocurrencies, payments may be made through other anonymous currencies, including payment cards. There is little research regarding where the proceeds of these crimes go once they depart the victims' possession: a problem that also affects the ability of the authorities to prosecute the fraudsters or recover the proceeds.

Typology of Transactions

The literature alludes to transactions that facilitate or are a part of several types of cybercrime; however, details and data are often scarce. In considering these transactions, we suggest a five-part typology: Willing, coerced, filched, laundering, and bartered transactions. In classifying transactions, we suggest a mechanism to understand how parties to the transactions understand their roles and how they choose to request or execute transactions.

Willing transactions

Willing transactions in a cybercrime context occur when both the payer and the payee are willing, knowledgeable participants getting, generally, what they expect, similar to ordinary, licit market transactions. Simply put, *willing transactions* typically involve payers/buyers purchasing illicit products or services and payees/sellers honouring their sales to the best of their abilities.

Within cybercriminal ecosystems, there are many products and services that are for sale with plenty of willing consumers. They include *inter alia*; stolen, counterfeit, or unregulated pharmaceuticals (R. Anderson et al. 2012; Katsuki, Mackey, and Cuomo 2015; Mackey and Liang 2011; Orsolini et al. 2015); illicit drugs (Aldridge and Décary-Hétu 2014, 2016; Barratt, Ferris, and Winstock 2014; Décary-Hétu, Paquet-Clouston, and Aldridge 2016; Demant et al. 2019); weapons (Chaudhry 2017); data, such as trade secrets, personal information, or credentials (SecureWorks 2016; Gaspareniene and Remeikiene 2015; McFarland, Paget, and Samani 2015; Zaytoun 2018); child exploitation materials (Hernandez et al. 2018), physical computer equipment and grey market services (Vidal and Choo 2018; Warren et al. 2017); malware (Broadhurst et al. 2018; Etaher, Weir, and Alazab 2015; Pastrana and Suarez-Tangil 2019; Bayoumy 2018); crime-as-a-service, such as DDoS attacks (Alazab and Broadhurst 2016; SecureWorks 2016; Ghernaouti-Hélie 2012); or financing an activity, such as a murder or terrorism (Carmona 2015; Carroll and Windle 2018).

Willing transactions may be negotiated and completed in a variety of spaces, including clearnet and darknet forums; private groups within social media platforms, such as Facebook (Demant et al. 2019); encrypted private communication channels, such as WhatsApp, Signal, QQ chat groups, Internet Relay Chat (IRC), or Jabber (XMPP) connections; and non-encrypted, commonly used systems, such as a commercial email provider or Skype (Hutchings and Pastrana 2019). The negotiation and completion of transactions may occur in distinct spaces; for instance, negotiations may start online and move offline for payment to be completed. This practice has been observed in illicit drug transactions where a connection is negotiated within a forum, but delivery occurs in person (Demant et al. 2019). It is also likely that state-sponsored cybercrime involves payment negotiations and completions that occur offline or via ordinary communication between employer and employee.

When considering online payments, the transacting parties’ expectations and accessibility to payment instruments are important. In cryptomarkets or forums, which may facilitate most of the buying and selling considered in the context of *willing transactions*, participants in any given transaction are likely to value anonymity and security, due to the illicit nature of the purchase and, particularly for new buyers, the uncertain delivery of the product or services purchased. To respond to these trust concerns, participants make transactions that often involve cryptocurrencies and escrow services (Janze 2017; Hutchings 2018; Weber and Kruisbergen 2019).

Bitcoin, which is pseudo-anonymous, has long been the dominant cryptocurrency accepted on and transacted within cryptomarkets. Bitcoin accounts for an estimated 40% of identified criminal-to-criminal payments (Paquet-Clouston, Haslhofer, and Dupont 2019). However, more recently, other cryptocurrencies, such as Zcash, Monero, and Dash have become more commonly transacted, given their superior anonymity (Kappos et al. 2018). The cryptocurrencies attackers choose to set as payment methods are likely a function of accessibility and, to a lesser extent, stability. Obscure cryptocurrencies are difficult to acquire and to cash out, meaning that most vendors will accept cryptocurrencies with higher market caps and common exchange presence. Moreover, obscure cryptocurrencies may be even more volatile than popular cryptocurrencies and carry the risk that they will cease (Wu, Wheatley, and Sornette 2018). While cryptocurrency profits may be reinvested in the criminal ecosystems (Carroll and Windle 2018) or spent directly on everyday goods and services as well as luxury items (Custers, Pool, and Cornelisse 2018), the cybercriminals must consider their capacity to cash out and spend proceeds of crime on products not available for purchase with cryptocurrencies.

Escrow services serve as guarantors for payment, thus underwriting trust, an often-necessary feature, given the irreversibility of most cryptocurrencies. For a percentage of the total payment transacted, escrow services hold payment for the buyer, releasing payment to the provider once the provider has fulfilled what it promised (Janze 2017; Hutchings 2018; Weber and Kruisbergen 2019). The role that escrow services played in building trust in anonymous marketplaces was the key for early darkweb marketplaces’ success (Pace 2017).

Cryptocurrency is not the only mechanism for *willing transactions* in cybercrime. Some payment transactions for illicit goods and services may use standard, regulated payment systems that transact fiat currency. Prior to darknet marketplaces, illicit drugs were sold via online informal bulletin boards that often included PayPal as a payment option (Böhme et al. 2015). In one study of the purchase of child exploitation materials and demand services in the Philippines, participants paid and received payments via PayPal or money transferring services, such as Western Union, Xoom (a PayPal service), Azimo, or GCash (Hernandez et al. 2018). A report on stolen corporate data stated that sellers accepted payment using QIWI or Yandex.Money, both legitimate and commonly-used Russian-based payment systems (SecureWorks 2016). These transactions may be favoured by the parties involved, despite the lack of anonymity they offer. Payers may appreciate the ease of access to send funds in fiat currency, while payees may appreciate how quickly the funds are received and their immediate access to money that they can use instantly. Until cryptocurrencies share those characteristics, they have a comparative disadvantage. Accordingly, given the use of these payment systems, which are ostensibly under the purview of regulatory bodies, a better understanding of their usage to facilitate the purchase of illicit goods needs to be developed.

Coerced transactions

Coerced transactions are transactions where payees/offenders compel or pressure payers/victims to pay. *Coerced transactions* may be in the form of payments solicited by payees via ransom, such as locking data through ransomware or stealing data and threatening to publish it (Abu, Lateef, and Echobu 2018; Böhme et al. 2015; Conti, Gangwal, and Ruj 2018; Irwin and Turner 2018); extortion, such as attacking a website with a sustained DDoS attack and asking payment to cease the interruption or claiming (often falsely) that the attackers have access to sexual content of the victim and will publish it (FBI 2017; Australian Government 2015; Digital Shadows Photon Research Team 2019); or social engineering (Samani and McFarland 2015; Rusch 1999), such as asking for money as a part of a romance scam (Whitty and Buchanan 2012), stranded traveller scam (R. Anderson et al. 2012), '419' scam (Boateng et al. 2011), business email compromise (FBI 2018, 2017, 2014), or the recruitment of unwitting money mules (Moiseienko and Kraft 2018; Galdo, Tait, and Feldman 2018; Aston et al. 2009; Leukfeldt and Jansen 2015). *Coerced transactions* may also be initiated by the payer who attempts to pay for products or services or attempts to participate in schemes that require investment – such as money or computer hardware (FBI 2014) – to participate, whereby the providers never honour their advertised commitments (Vasek and Moore 2018; Akanle, Adesina, and Akarah 2016).

Coerced transactions that result from extortion or ransom often use cryptocurrencies or, to a lesser extent, prepaid payment cards or vouchers. Victims will engage with these payment platforms, which are likely to be unusual to them, because they wish to recover their data or end an attack. As a result, attackers, who are realistic in terms of the capacity of their victims, favour Bitcoin, which is by far the most accessible cryptocurrency to a lay consumer. Some ransoms have been requested in prepaid payment cards. Alternative cryptocurrencies have been requested as well. For example, Dash has been demanded in more recent ransomware campaigns, notably GandCrab; however, in this case, Bitcoin was later made an additional payment option to encourage more victims to pay their ransom (Kujawa et al. 2018). (In this case, the offenders may have overestimated the technical competence of their targets.)

While DDoS extortion still appears to have some degree of success (Mansfield-Devine 2015; Ibragimove et al. 2018; Akamai 2019), recent ransomware appears not to be consistently successful as operational security improves, including improved backup systems and a general refusal of the public to pay out ransoms. In response, ransomware attacks appear to have evolved to focus on larger, specific targets that hold a lot of sensitive data, such as municipalities and health service providers, that occasionally continue to pay out large ransoms (Slayton 2018; De Groot 2019; Irwin and Dawson 2019; Paquet-Clouston, Haslhofer, and Dupont 2019; O'Brien 2017; Irwin and Turner 2018; Kujawa et al. 2018).

Given the uneven success of ransomware, cybercriminals have begun to innovate new strategies to generate revenue. Notably, cryptojacking operations have recently increased, given the decreased likelihood of being captured and increased success in generating revenue (Zimba, Wang, and Mulenga 2019). Another innovation involves asking victims for ransom with the threat of exposing sensitive data instead of encrypting it (Head 2019; Mandiant 2016), and engaging in other forms of blackmail (FBI 2014). Yet another innovation involves holding fraudulent crowdsourcing campaigns to defraud investors and/or potentially to launder the proceeds of crime by creating points where illicit funds can be consolidated without delivering on a promised product, an action that is relatively common on most crowdsourcing platforms and one that does not face a mechanism to police abuse (Flashpoint 2016).

Unlike ransoms and extortions, socially engineered *coerced transactions* will most likely use the currency that the victim expects to be using. Social engineered scams that target individuals will likely use fiat transactions through bank transfers or transfer services, such as Western Union, since the victim expects to pay the money in that form. Using alternative payment methods, that may fall outside the routine of the victim, is more likely to cause the victim concern (by making them wonder if all is as it seems) or put the victim in a position where s/he cannot complete the transfer due to a lack of access or ability to access the alternative payment system. The role of expectations is likewise apparent when corporations are the target; business email compromise results in bank transfers, since requesting payment in an unusual means would raise suspicion and result in the scam being more likely to be detected by the victim.

Setting aside the thefts of cryptocurrencies by exchange managers or hackers, fiat currencies represent the highest proportion of stolen currency facilitated by cybercrime, though the transfers themselves often occur via ordinary, licit, and regulated fiat currency transfer systems. The literature indicates that offenders operate with knowledge of regulatory limits, transacting in amounts that allow them to collect funds without identification (Ogwezzy 2012), and spend money on cards that will not trigger any serious investigation (Brenig, Accorsi, and Müller 2015). Moreover, successful offenders understand how to trigger transactions that are difficult to chargeback/reverse, even within regulated systems, ensuring that once offenders receive the money, victims will struggle to recover it even if they realise they have been scammed (Remorin, Flores, and Matsukawa 2018; Mansfield-Devine 2016). Such bank and regulatory requirements can change over time, and there has been little research on the ways in which offenders circumvent (or fail to circumvent) these shifting anti-money laundering processes.

Filched transactions

Filched transactions in a cybercrime context are transactions where offenders steal money or digital assets from their victims. The victims are typically unaware of the theft until after it occurs. Thefts may be of physical fiat currency, such as ATM jackpotting (CASIS Vancouver 2018); digital fiat currency, such as bank account thefts or ACH/SWIFT compromises (SWIFT 2019; Federal Reserve Board 2018; Europol 2013; Moiseienko and Kraft 2018; Etaher, Weir, and Alazab 2015); unauthorised card use/card fraud, or unauthorised credential/account use (Federal Reserve Board 2018; Jianwei, Liang, and Haixin 2012; R. Anderson et al. 2012; Europol 2013; Etaher, Weir, and Alazab 2015); cryptocurrency and virtual currency, such as breaches of cryptocurrency exchanges (Bischoping 2018; Campbell-Verduyn 2018; Guerrero-Saade and Moriuchi 2018); exit scams (Janze 2017; CipherTrace 2019a), or the theft of video game currency or assets (Xie 2019; Seok and DaCosta 2019; Burns 2011; Patterson and Hobbs 2010; Chung et al. 2006); or resources, such as the case of cryptojacking, where attackers use the victim’s computer resources to mine for cryptocurrency without sharing the proceeds with the victim (Zimba, Wang, and Mulenga 2019; Pastrana and Suarez-Tangil 2019; Check Point 2019).

Filched transactions are often opportunistic, targeting organizations and people who have vulnerabilities in their virtual products or operational security. Attackers, including state actors such as North Korea (Carlisle and Izenman 2019; Guerrero-Saade and Moriuchi 2018), have targeted cryptocurrency exchanges and initial coin offerings (ICOs) throughout the world (Bratspies 2018; Bott and Milkau 2016; Bayoumy 2018; Corbet et al. 2018). The speed at which some of these services come to market likely means a lack of robust security measures. Even in the cases of standard security measures, such as two-factor authentication (2FA), attackers have developed strategies to circumvent such measures (Adham et al. 2013). One example is SIM swapping that allows attackers to gain access to the phone services of a victim, thus allowing the attacker to confirm the 2FA and gain unrestricted access to the account (CipherTrace 2019a). Insider theft in exchanges and darknet marketplaces is another significant threat (CipherTrace 2019a; Bayoumy 2018). Successful attacks, insider thefts, and exit scams often have resulted in significant, unrecoverable losses estimated to be in the tens and hundreds of millions of dollars at market rates (Bischoping 2018; Avdoshin and Lazarenko 2018; Barnes 2018; Campbell-Verduyn 2018; Chainalysis 2018).

In addition to directly stealing money, offenders employ data theft, often through the use of phishing attacks or the deployment of trojans (Etaher, Weir, and Alazab 2015; Guri 2018; Aston et al. 2009), to gain personal identifying information (PII), payment information, login credentials, or other sensitive data. This data then facilitates future theft. One strategy is to spoof websites, such as eBay, PayPal, or legitimate financial institutions' websites, and to have victims enter sensitive data, which attackers then use to set up unauthorised accounts or make unauthorised payments (Cárdenas et al. 2009). Lower-tech solutions, that continue to be employed, include the use of skimming devices placed on ATM machines (FTR Team and European Cybercrime Centre 2017).

In one sector where the literature appears to indicate that filched transactions have decreased is the banking industry. The banking industry has improved its operational security which has resulted in an increased capacity to protect against fraud and theft using their systems. For instance, despite early prevalence of ACH fraud/unauthorised usage, the ACH system has improved to the point where it has one of the lowest fraud rates of existing payment options; ACH compromises are far less likely to be successful and to pay out attackers (Federal Reserve Board 2018; McCartney 2017). The same is true within the SWIFT system (SWIFT 2019).

In short, in cyberspace, as is the case in offline applications, opportunity still makes the thief (Felson and Clarke 1998), though not all thieves have the knowledge or imagination to take the opportunities on offer. Filched transactions vary in terms of their objectives, stealing money and data, which can then be monetised. Moreover, thieves may steal small amounts from several victims, or they may target big windfalls from specific victims. It is clear, however, that so long as attackers can identify weaknesses in operational security and so long as attribution remains low and often slow, potential victims need to continue to invest in preventative methods and develop potentially better systems that allow them to track digital transactions, particularly those that occur within regulated financial systems.

Laundering transactions (and transactional facilitators)

Laundering transactions are transactions that obfuscate the origin of the proceeds of a crime or successfully cash out those proceeds into apparently legitimate, spendable currency. In the context of cybercrime, *laundering transactions* may include moving currency in and out of different currency types or via accounts in an attempt to hide the provenance of either fiat or cryptocurrency; directly paying for goods and services; or cashing the money out to be able to spend it without suspicion. Although the cybercrime literature understandably focuses on the laundering of cryptocurrency, money launderers use a variety of facilitators and techniques, examined throughout this section. While it is possible to launder the proceeds of offline crime using online means – indeed it is arguable that all electronic transfers are ‘cyber-enabled’ or at least ‘cyber-assisted’ - traditional laundering techniques are likely to remain more effective so long as cash and fiat currency retains its marked advantage in terms of market acceptance for settling debts and for payment for licit goods and services. Accordingly, in this section, we focus on the laundering of the proceeds of cybercrime and cyber-assisted crime.

When money is stolen at volumes larger than what can be ‘reasonably’ spent or where the offenders wish to save part or all of their crime proceeds, it must be laundered (Levi and Soudijn, 2020). There are several strategies that money launderers (including predicate offenders who self-launder) use to convert the proceeds of their cybercrimes into laundered money that can be spent without suspicion. Money launderers take into account regulatory frameworks and the capacity of investigative bodies, innovating strategies to avoid detection (W. Buchanan, Dyson, and Bell 2018).

Moreover, money launderers may use several transactional facilitators to clean the proceeds of their crimes.

Money Mules

Money mules are a common device used by money launderers to launder fiat currency especially digital fiat currency. The mules receive a deposit into their accounts and then forward that money on to another account, sometimes, but not always, keeping a fee for themselves (or in exchange for repaying a debt). Launderers typically recruit money mules in two ways: as unwitting accomplices or as willing and knowing accomplices (Button and Cross 2017). Offenders will manipulate unwitting mules to engage in illicit behaviours without realizing they are engaging in an illicit act. These activities may include *inter alia*, serving as an intermediary, delivering a stolen good, or transferring money under the guise of an ostensibly benevolent act, such as supporting someone in need overseas, with the mules keeping little or nothing for themselves (Button and Cross 2017), or in the capacity of a job, typically advertised as a work-from-home scheme (Aston et al. 2009).

Complicit mules engage in similar behaviours, but with the knowledge that their behaviour is illicit. For instance, they may use their own accounts to conduct wire transfers and keep a fee; use stolen identities to create new accounts from which they can transfer money or access compromised accounts with stolen credentials (Bayoumy 2018; FBI 2018; Custers, Pool, and Cornelisse 2018); collect money from an jackpotted ATM or cryptoasset ATM and deliver or deposit those funds to a secure point accessible to the fraudsters with whom they are colluding (Elliptic 2019; CASIS Vancouver 2018; FTR Team and European Cybercrime Centre 2017; Broadhurst et al. 2014). The general literature on money muling is not concerned specifically with cryptocurrencies at any stage in the transaction cycle: but inasmuch as funds are wire transferred, this makes it at least cyber-assisted or cyber-enabled crime. In 2019, new asset freezing order powers were used by the UK authorities to clamp down on Chinese accounts used as a conduit for allegedly illicit funds, a concern also expressed in other countries such as the US and Australia, though the proportionate extent to which these related to cybercrime, organised crime, corruption or simply circumventing Chinese exchange control rules is unknown, either to researchers or to the NCA.[17]

Launderers often recruit several money mules and have them transact among themselves. This strategy makes the money mule a cutout, a person who becomes the low-hanging fruit that law enforcement arrests when investigations are successful

(Gundur 2019), but who is unable to further identify the ‘core’ money launderer (Galdo, Tait, and Feldman 2018) or the predicate offender(s).

Banks and Money Transmission Businesses

Banks play a significant role in money laundering throughout the world, and some of their innovations, such as the capacity to open a bank account online (rather than at a branch, in person) is leveraged by money launderers. Banks in regions with lax regulatory frameworks and enforcement are especially susceptible to being used by money launderers (W. Buchanan, Dyson, and Bell 2018). Historically, and into the present, money launderers have created accounts using stolen (or perhaps more accurately, borrowed or duplicated) identity information, allowing them to create shell accounts through which they can transfer money, without affecting the finances or alerting the individual whose identity was used to initialise the account (J. Buchanan and Grant 2001; Wall 2013). Indeed, if we kept data on every fraud case in which ‘stolen’ ID was used to open accounts, then it might lead us to question the validity of some anti-money laundering controls. In some dated cases in Taiwan, criminals used a compromised bank network to conceal the source of the income they were laundering and then disguised the income within the bank’s ledger system to make it appear legitimate (Chung et al. 2006). More recent bank manipulations were reported in European and Middle Eastern financial institutions (Mandiant 2017). Frauds that occur in developing regions where regulation may be poorer or more poorly enforced often leverage banking insiders to facilitate illicit transactions or law enforcement to turn a blind eye to illicit behaviour (Boateng et al. 2011; Aransiola and Asindemade 2011; Ibrahim 2016).

Banks and payment systems play a significant role in fraud detection. Efforts put into place by banks and payment systems to examine their clients and outbound transfers, and to communicate concerns within their networks are the most effective means to curb fraudulent transfers (SWIFT 2019; Hileman and Rauchs 2017). When banks do not engage in this role, they are more easily leveraged for laundering purposes. Similarly, the capacity and/or willingness of money transmission businesses to detect or pursue fraud determine their viability in the money laundering ecosystem. Money transmission businesses, like Western Union and Money Gram, are often used by offenders to receive money because the combination of an ID and pin number requested from the victim is enough to receive the transfer, and because their networks of stores are ubiquitous globally. Transfers below certain thresholds may not even require ID and low-value losses are unlikely to be investigated by the company or certainly not by law enforcement, unless it is thought to be terrorism-related.

Emerging transaction systems, including mobile money like M-Pesa, mobile payment platforms like AliPay, and remittance systems such as Abra (Wörner et al. 2016), are, in some cases, replacing cash transactions as the primary means of payment. These systems present further opportunities for money laundering. While there are reports of these payment systems being attacked (McGuire 2018), the extent to which money laundering of proceeds beyond these cyber-attacks occurs through them is still largely unknown.

Additionally, there is an increasing number of technologies that facilitate the transaction of both fiat and virtual currency. Some have come and went; others appear to be gaining enough steady, common usage to persist in the marketplace. These include platforms, such as now defunct Kipochi Limited in Kenya, which was used to buy and sell cryptocurrency with mobile payment credits (Bissessar 2016; Sirila 2014); and platforms, such as BitPesa in Kenya and Abra in the United States and Philippines, that allow individuals to pay in cryptocurrency for items sold in fiat currency or mobile money or to remit money to individuals abroad in fiat currency (Cotton 2018; Bissessar 2016). There are also new technologies proposed, such as *Libra* (Libra Association Members 2019), that may (or may not) disrupt payment systems over time. However, there is little information regarding how these payment systems are currently leveraged for money laundering purposes. If these platforms manage to persist and gain steady usage, they could be leveraged to conduct high volume, low value transactions that would allow launderers to move money below thresholds of detection and investigation, if that were feasible depending on the scale and regularity of the criminal money transfer needs. Much depends upon the direction of recognition and regulation of cryptocurrencies, which is a dynamic policy issue transnationally.

What is certain is that several money transmission businesses have been used to transmit and launder money. Defunct, but previously popular systems include E-Gold and Liberty Reserve, both of which had non-existent KYC standards. Systems such as WebMoney and Perfect Money still operate, with varying degrees of claimed compliance.

Virtual currency laundering

Europol estimates that about 3% to 4% of Europe’s crime proceeds are laundered using cryptocurrencies (the rest is mostly using cash) and states that cryptocurrencies are a means through which proceeds of crime are transacted across borders, particularly to circumvent exchange controls (R.J. Anderson, Shumailov, et al. 2019). This reflects intelligence reports to which they have access, rather than being an established figure. (Within the Eurozone, there is no problem of needing to circumvent such controls, since there is a common currency. Proceeds of crimes from countries with exchange controls can be laundered in the EU and in the UK, as elsewhere.) Nonetheless, the literature focuses primarily on the laundering of proceeds of cyber-assisted or cyber-dependent crime. Notably, laundering cryptocurrency is not perfectly analogous to fiat currency money laundering strategies that have the three distinct steps of placement, layering, and integration (Ajello 2014), though this three-stage model has been criticised as applicable only in some restricted contexts (Levi and Soudijn 2020). Cleansing funds within a cryptocurrency's blockchain typically requires fewer steps; much of the placement, layering, and integration all occurs within the cryptocurrency's financial ecosystem (Fanusie and Robinson 2018). Nonetheless, while it logically follows that if a cybercrime is transacted in cryptocurrency, cryptocurrency will be part of the laundering process, if there is a cashout, the laundering process may occur using fiat currency.

Laundering cryptocurrency is a small volume activity. However, it does appear that it has some success. Fast attribution remains a problem given the rapid dispersal of assets once stolen (Bischoping 2018). Some commentators note that cryptocurrencies have a great potential to being transported at volume with small physical dimensions and to being transacted relatively quickly (Bååth and Zellhorn 2016; Ajello 2014). Despite these attributes, though it should not be assumed that all criminals are well informed and sophisticated, rational launderers still must seek to obfuscate the provenance of their proceeds of crime since pseudo-anonymity cannot guarantee non-traceability. Accordingly, money launderers seek to create cutouts for their transaction chains. A cutout is a mechanism that impedes an investigator's capacity to understand how two parties of a transaction are related.

Nevertheless, laundering cryptocurrency is not necessarily a fool proof process, and cutouts are not built into most transactional relationships. For instance, Bitcoin's pseudo-anonymity renders it a dangerous tool for laundering money (Bistarelli, Mercanti, and Santini 2018). Even as Bitcoin passes through tumblers, i.e. websites that claim to mix cryptocurrencies in a variety of ways in an attempt to obfuscate their origin, there are techniques that allow investigators to identify which Bitcoins were used in illicit transactions (R.J. Anderson, Shumailov, et al. 2019). (Though it should not be assumed that law enforcement will actually follow up either the predicate crimes or the laundering process, so much careless behaviour will go unpunished.)

Once at least some money launderers understood these risks, they diversified their obfuscation strategies. In some cases, money launderers employed tellers to assist in transferring illicit proceeds through digital currency services and in and out of fiat currencies (Broadhurst et al. 2014). One study determined that thieves funnel (likely using automated techniques) stolen funds through a complex array of wallets and exchanges, transferring funds at least 5,000 times (Chainalysis 2019). However, given the analysis, it is clear that even complex, high-volume transacting patterns can be traceable. In response, one mixer, Bitmixer, engages in a process of cryptodusting whereby it taints as many coins as possible, to increase the rate of false positives of coins associated with criminal events (CipherTrace 2019a). Moreover, it must be noted that an increasing proportion of transactions happen off-chain, due to its speed and cost savings, whereby an exchange credits their clients' ledgers without actually making a blockchain transaction on their clients' behalf, thus potentially rendering some transactions harder to trace (Zaytoun 2018; Poon and Dryja 2016).

A small proportion (0.67%) of overall funds that flow through Bitcoin exchanges and other conversion services have an illicit provenance, and it appears that the proportion of illicit funds transacted decreased from 2014 to 2016 (Elliptic 2019). AML/CTF controls appear to have an impact on where illicitly obtained virtual currencies are transacted, with US exchanges that were subject to earlier controls being less popular than European exchanges (Elliptic 2019). The implementation of AML/CTF standards across European exchanges will likely result in illicit users displacing to exchanges under laxer regulatory regimes.

Notably, specific exchanges, mixing services, and online gambling sites appear to handle disproportionate amounts of Bitcoin laundering, regardless of how the Bitcoin was illegally obtained (Fanusie and Robinson 2018). Exchanges of note are the defunct BTC-e, linked to the laundering of the Mt. Gox theft (Putong, Kainde, and Astuti 2018), and HitBTC, linked to the laundering of the Wannacry ransoms (R.J. Anderson, Shumailov, et al. 2019).

Another reported technique used to launder cryptocurrency involves transferring cryptocurrencies into other cryptocurrencies, a process known as "chain hopping" (Moiseienko and Kraft 2018). These types of transactions can occur in licit exchanges and are not subject to regulatory oversight. However, apart from skill barriers to entry for less cyber-competent offenders, chain hopping still presents potential traceability and functionality problems, particularly given the low adoption rate of altcoins

(Bissessar 2016). One privacy researcher (Sarah Jamie Lewis, personal correspondence) pointed out the following in reference to chain hopping:

> First, the cross-blockchain transfer still has to take place. The only viable anonymous way (i.e. not using a centralised exchange - which would require KYC information) would be using something like Bisq[18] which has a natural cap on how much you can transfer. Even worse [in terms of preserving anonymity] would be atomic swaps[19] which would leak artefacts referencing both sides of the transaction on the blockchain. (It would likely be easier to convert to cash and simply buy altcoins on a market, under the assumption that going from bitcoin into cash can be pretty private).
>
> Second, each respective blockchain has a timestamped indication of the transfer, so if one knows, or hypothesizes, that such a transfer took place then it would not be too hard to look for movements of significant value from one blockchain to a number of candidates.
>
> Third, getting the money out of non-bitcoin blockchains presents increased difficulties – [while] bitcoin-to-cash services/ATMs can be found in a number of cities, the same is not true of a number of others (particularly for privacy coins which I would speculate would be the destination of choice).
>
> Fourth, [instead of chain hopping] techniques like CoinJoin[20] would likely offer far better ways to hinder tracing, and the tools exist today that make it accessible and useable (at least to those with an increased motivation).

Launderers have also used gaming platforms to launder money (Levi 2013), though unless KYC vigilance levels are low and/or the firm is run by crooks, gaming is a difficult mechanism for laundering large or regular amounts. These platforms include video gaming ecosystems, where they may purchase tokens, game currency, or game assets, and trade or resell them (Moiseienko and Izenman 2019). A recent study in British Columbia found that casino tokens were used as a currency for Chinese funds transfers, whether from mainstream crimes and/or to evade Chinese currency controls (German 2018). Gambling platforms are also used to launder money. Here, launderers buy credit using virtual currency to gamble with, take (generally speaking) their losses, and then cash out the remainder into fiat currency as gambling winnings which is then spendable income (Fanusie and Robinson 2018; Brooks 2012; Choi 2018; Fiedler 2013; McMullan and Rege 2010).

Overall, regarding the laundering of cryptocurrencies, despite technological improvements and wider acceptability, it appears that the transactions using these currencies are difficult to scale without unavoidable risk. The volume of similar, licit, transactions may make detection difficult (Brooks 2012), resulting in a reality where whether an offender is caught is a function of law-enforcement’s capacity to investigate these transactions (Egan 2018). Ultimately, it is possible that the limitations present in laundering cryptocurrencies are such that opportunities are more “perceived than real” (Campbell-Verduyn 2018, 288), at least for many offenders and even for some professional launderers. An important distinction in all money laundering is whether the laundering is part of the crime (as in many frauds) or is a separate part of the crime script, in other words the laundering is of the crimes of others. In any event, given that many ‘service crimes’ like drugs and people trafficking/retail sales are for cash, crypto-laundering needs to be supplemented with an understanding of how cash is translated into cryptocurrencies.

Cashing Out

Criminal actors eventually will want to cash out and spend at least a portion of the proceeds of their crime. This is true for individuals, groups, and state actors, all of whom engage in cashing out activities (Elliptic 2019), and this is true whether the money possessed is fiat or virtual currency.

Fiat currency may be transacted using a series of compromised bank accounts, a network of companies that devolves payments to money mules (Moiseienko and Kraft 2018), or direct Western Union/ MoneyGram transactions that deliver the funds to a point that the offender has access to (Custers, Pool, and Cornelisse 2018; MacRae and Franqueira 2017). Fiat currency may be spent in a variety of forms, such as buying digital assets (Elliptic 2019), gambling (Brooks 2012; Fiedler 2013; Gainsbury and Blaszczynski 2017), purchasing luxury goods (Custers, Pool, and Cornelisse 2018), or buying airline tickets (Hutchings 2018). Additionally, other ways to cash out stolen fiat currency include direct purchases of every-day goods and services that the purchaser benefits from (Ogunbadewa 2013; Custers, Pool, and Cornelisse 2018), such as airline/hotel points (SecureWorks 2016), PayPal payments (Hutchings and Pastrana 2019), gift cards, or gifts directed to another account on platforms, such as the now defunct money transferring platform Tendr or the fundraising platform PayItSquare, that may be a front for the scammer (Flashpoint 2016). Some cashout services are also advertised in illicit marketplaces, with a variety of solutions offered, including “guides, to actionable solutions, like PayPal or bank account access” (Van Wegberg, Oerlemans, and van Deventer 2018).

Virtual currencies may be cashed out in similar ways at modest volumes, particularly when there are services that allow for the near-instantaneous conversion of cryptocurrency into fiat currency to pay vendors (Custers, Pool, and Cornelisse 2018; McGuire 2018), an increasing number of whom is accepting cryptocurrency (Mikhaylov and Frank 2016; Agari Cyber Intelligence Division 2019; FTR Team 2015). Some explicit cashout services exist, which accept dirty cryptocurrency in exchange for stolen goods or payment cards (Fuentes 2017). Other cashout services are, in fact, scams (Vasek and Moore 2015).

For some cybercriminals, cashing out quickly is not an imperative. Holding cryptocurrency to see if it improves its value may be a rational action. However, while some virtual proceeds can be held almost indefinitely, doing so is risky, particularly if one relies on unregulated exchanges and wallet services which have a history of closing, whether from fraud by the their founders, their exchanges, law enforcement operations or simply from changes in the economic environment. Accordingly, it is likely that cyberoffenders will convert at least some of the proceeds of crime into fiat currency or needed goods or services.

Large volume cashouts of cryptocurrency are also likely to happen. Large volume cashouts of illicitly acquired cryptocurrency almost certainly leverage relationships with exchanges or banks that are in poorly regulated locations or locations where corruption is easily attained (though if corruption means that the bank itself becomes risky or a domestic or international enforcement target, the funds may be lost). North Korea, for example, maintains a network of transfer points throughout Southeast Asia, though it may avoid cashing out large sums to reduce attention (Carlisle and Izenman 2019). In addition, there exist some specialised money laundering brokers, such as the Chinese Underground Banking Systems (CUBS), that appear to be capable of laundering relatively large sums of money in both fiat and digital currency – presumed to be millions of dollars (CipherTrace 2019b).

Bartered transactions

Bartered transactions occur when two parties exchange goods and/or services. Such transactions have been observed within child exploitation networks that trade in exploitation material (A. Carr 2013; Burgess et al. 2008), and through some payment requests by vendors of illicit software whereby sellers ask for compensation via prepaid payment cards or payment codes (Hernandez et al. 2018; FTR Team 2015; Urano 2015). These transactions are difficult to monitor, interrupt, or investigate. While they represent a relatively small proportion of cybercrime-related transactions identified in the literature, *bartering transactions* could be a means that cybercriminal traders develop further to evade detection if regulation makes proceeds generated by other methods of payment more difficult to launder and cash out. However, absent a criminal equivalent of Amazon Marketplace, bartering depends on direct P2P exchanges of mutually desired resources that may be a hassle to negotiate in the short or long run for most offenders.

Conclusion

This section has surveyed the state of cybercrime in countries that use English as an administrative language and have a significant population of internet users. It has shown the variation of capacity between well-resourced countries and developing countries. It has discussed the various financial ecosystems that are in operation and how cybercrime impacts upon them. It has provided an overview of the state of regulation and, to an extent, cooperation in the English-speaking world in the surveys set out in this report. It has provided a series of possible scripts to help understand criminal ecosystems, taking note of the dangers of focussing too heavily on crypto-currency components of crime and of under-playing the importance of more modest technological tools such as smartphones. It has developed a typology of transactions and used examples from the literature to illustrate them. With this exercise, we have shown that intentionally or as an unintended side-effect of journal and publisher preferences, the literature does a poor job of recording specific details and maintaining an up-to-date ongoing record of how transactions unfold vis-à-vis cybercrime. We suggest that an ongoing exercise that monitors these types of transactions would be helpful for law enforcement and regulators, given that virtual transactions are an increasing proportion of all transactions and that emerging and disruptive technologies invariably change the way in which people engage with one another.

Works Cited

Ablon, Lillian, Martin C Libicki, and Andrea A Golay. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: Rand Corporation.

Abu, SO, OM Lateef, and J Echobu. 2018. "Determinants of Cyber Fraud Investigation in Nigeria."

Adams, John. 2016. *Canada and Cyber*. Canadian Global Affairs Institute.

Adham, Manal, Amir Azodi, Yvo Desmedt, and Ioannis Karaolis. 2013. "How to Attack Two-Factor Authentication Internet Banking." International Conference on Financial Cryptography and Data Security.

Adomi, Esharenana E, and Stella E Igun. 2008. "Combating Cyber Crime in Nigeria." *The Electronic Library* 26 (5): 716-725.

Agari Cyber Intelligence Division. 2019. *Scarlet Widow Bec Bitcoin Laundry: Scam, Rinse, Repeat - Part 2: Nigeria-Based Scammer Group Targets Nonprofits and Schools; Launders Stolen Gift Cards through Online Cryptocurrency Exchanges*. Foster City, CA: Agari Data, Inc.

Ajello, Nicholas. 2014. "Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege against Self-Incrimination." 80: 435.

Akamai. 2019. *[State of the Internet]/ Security DDOS and Application Attacks Report*. Vol. 5. Vol. 1: Akamai.

Akande, Tunji. 2014. "Youth Unemployment in Nigeria: A Situation Analysis." *Ibadan: NISER, Brookings Institute Report*. https://www.brookings.edu/blog/africa-in-focus/2014/09/23/youth-unemployment-in-nigeria-a-situation-analysis/.

Akanle, Olayinka, JO Adesina, and EP Akarah. 2016. "Towards Human Dignity and the Internet: The Cybercrime (Yahoo Yahoo) Phenomenon in Nigeria." *African Journal of Science, Technology, Innovation and Development* 8 (2): 213-220.

Akomea-Frimpong, Isaac, Charles Andoh, Agnes Akomea-Frimpong, and Yvonne Dwomoh-Okudzeto. 2019. "Control of Fraud on Mobile Money Services in Ghana: An Exploratory Study." *Journal of Money Laundering Control*.

Alazab, Mamoun, and Roderic Broadhurst. 2016. "Spam and Criminal Activity." *Trends and Issues in Crime and Criminal Justice (Australian Institute of Criminology)* (52).

Aldridge, Judith, and David Décary-Hétu. 2014. "Not An'ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation." *Available at SSRN 2436643*. http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2436643.

---. 2016. "Hidden Wholesale: The Drug Diffusing Capacity of Online Drug Cryptomarkets." *International Journal of Drug Policy* 35: 7-15.

Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2012. "Measuring the Cost of Cybercrime." https://doi.org/10.1007/978-3-642-39498-0_12.

Anderson, Ross, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. "Measuring the Changing Cost of Cybercrime."

Anderson, Ross John, Ilia Shumailov, Mansoor Ahmed, and Alessandro Rietmann. 2019. "Bitcoin Redux."

Antonakakis, Manos, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, and Michalis Kallitsis. 2017. "Understanding the Mirai Botnet." 26th {USENIX} Security Symposium ({USENIX} Security 17).

Arango-Arango, Carlos A, Yassine Bouhdaoui, David Bounie, Martina Eschelbach, and Lola Hernandez. 2018. "Cash Remains Top-of-Wallet! International Evidence from Payment Diaries." *Economic Modelling* 69: 38-48.

Aransiola, Joshua Oyeniyi, and Suraj Olalekan Asindemade. 2011. "Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria." *CyberPsychology, Behavior, and Social Networking* 14 (12): 759-763.

Arnold, Brent J. 2018. "Cyber Security in Canada: Structure and Challenges." *Governing Cyber Security in Canada, Australia and the United States,* edited by Christian Leuprecht and Stephanie MacLellan. Waterloo, Ontario: Centre for Internatinoal Governance Innovation.

Aston, Manuel, Stephen McCombie, Ben Reardon, and Paul Watters. 2009. "A Preliminary Profiling of Internet Money Mules: An Australian Perspective." 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing.

AUSTRAC. 2018a. *Austrac Annual Report*. Canberra: Government of Australia.

---. 2018b. "Criminal Threat Environment." Austrlian Government. Last Modified 11 April. https://web.archive.org/web/20190326080820/http://www.austrac.gov.au/superannuation-risk-assessment-threat.

---, 11 April, 2018c, "New Australian Laws to Regulate Cryptocurrency Providers," https://web.archive.org/web/20190326080351/http://www.austrac.gov.au/media/media-releases/new-australian-laws-regulate-cryptocurrency-providers.

Australian Crime Commission. 2018. *The Costs of Serious and Organised Crime in Australia 2013-14*. Canberra: Commonwealth of Australia.

Australian Cyber Security Centre. 2017. *Threat Report*. Canberra: Australian Government.

Australian Government. 2015. *ACSC Australian Cyber Security Centre 2015 Threat Report*. Canberra: Australian Government.

Australian Security Intelligence Organisation. 2018. *ASIO Annual Report*. Canberra: Australian Government.

Australian Security Intelligence Organisation. 2020. *ASIO Annual Report*. Canberra: Australian Government.

Avdoshin, SM, and AV Lazarenko. 2018. "Bitcoin Users Deanonymization Methods." 30 (1).

Bååth, David, and Felix Zellhorn. 2016. How to Combat Money Laundering in Bitcoin? An Institutional and Game Theoretic Approach to Anti-Money Laundering Prevention Measures Aimed at Bitcoin.

Bada, Maria, Basie Von Solms, and Ioannis Agrafiotis. 2018. "Reviewing National Cybersecurity Awareness in Africa: An Empirical Study."

Baggett, Ryan K, and Brian K Simpkins. 2018. *Homeland Security and Critical Infrastructure Protection*. Santa Barbara, CA: ABC-CLIO.

Ballou, TM, Joseph A Allen, and KK Francis. 2016. "Us Energy Sector Cybersecurity: Hands-Off Approach or Effective Partnership?" *Journal of Information Warfare* 15 (1): 44-59.

Barnes, Paul. 2018. "Cryptocurrency and Its Susceptibility to Speculative Bubbles, Manipulation, Scams and Fraud."

Barratt, Monica J, Jason A Ferris, and Adam R Winstock. 2014. "Use of Silk Road, the Online Drug Marketplace, in the United Kingdom, Australia and the United States." *Addiction* 109 (5): 774-783.

http://onlinelibrary.wiley.com/store/10.1111/add.12470/asset/add12470.pdf?v=1&t=i7hpycug&s=0f220bcb6c250f8d625a229fdd979c6fe461da57.

Bayoumy, Yara. 2018. "Cybercrime Economy: A Netnographic Study on the Dark Net Ecosystem for Ransomware." NTNU.

Beauregard, Eric, Jean Proulx, Kim Rossmo, Benoît Leclerc, and Jean-François Allaire. 2007. "Script Analysis of the Hunting Process of Serial Sex Offenders." *Criminal Justice and Behavior* 34 (8): 1069-1084. https://doi.org/10.1177/0093854807300851.

Bech, Morten L, Umar Faruqui, Frederik Ougaard, and Cristina Picillo. 2018. "Payments Are a-Changin’ but Cash Still Rules." *BIS Quarterly Review, March*.

Beech, Anthony R, Ian A Elliott, Astrid Birgden, and Donald Findlater. 2008. "The Internet and Child Sexual Offending: A Criminological Review." *Aggression and Violent Behavior* 13 (3): 216-228.

Bischoping, Gregory. 2018. "Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016." 167: 239.

Bissessar, Shiva. 2016. "Opportunities and Risks Associated with the Advent of Digital Currency in the Caribbean."

Bistarelli, Stefano, Ivan Mercanti, and Francesco Santini. 2018. "A Suite of Tools for the Forensic Analysis of Bitcoin Transactions: Preliminary Report." European Conference on Parallel Processing.

Bistarelli, Stefano, Matteo Parroccini, and Francesco Santini. 2018. "Visualizing Bitcoin Flows of Ransomware: Wannacry One Week Later." ITASEC.

Blakstad, Sofie, and Robert Allen. 2018. "Central Bank Digital Currencies and Cryptocurrencies." In *Fintech Revolution*, 87-112. Springer.

Bleakley, Paul. 2018. "Watching the Watchers: Taskforce Argos and the Evidentiary Issues Involved with Infiltrating Dark Web Child Exploitation Networks." *The Police Journal*: 0032258X18801409.

Blumenfeld, Matthew, Michael Horn, Keaghan Ames, Nikhil Raina, Cesar Munoz, and Margaret Paulsen. 2018. *Carving up Crypto: Regulators Begin to Find Their Footing.Regulatory Brief*: PriceWaterhouse Coopers.

Boateng, Richard, Longe Olumide, Robert Stephen Isabalija, and Joseph Budu. 2011. "Sakawa-Cybercrime and Criminality in Ghana." *Journal of Information Technology Impact* 11 (2): 85-100.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29 (2): 213-38.

Bott, Jürgen, and Udo Milkau. 2016. "A Market for Payments: Payment Choice in the 21st Century Digital Economy." In *Transforming Payment Systems in Europe*, 1-27. Springer.

Bottazzi, Giovanni, and Gianluigi Me. 2014. "The Botnet Revenue Model." The 7th International Conference on Security of Information and Networks, Glasgow.

---. 2015. "A Survey on Financial Botnets Threat." International Conference on Global Security, Safety, and Sustainability.

Bougaardt, Gino, and Michael Kyobe. 2011. "Investigating the Factors Inhibiting SMEs from Recognizing and Measuring Losses from Cyber Crime in South Africa." ICIME 2011-Proceedings of the 2nd International Conference on Information Management and Evaluation: ICIME 2011 Ryerson University, Toronto, Canada, 27-28 April 2011.

Bouveret, Antoine. 2018. *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. International Monetary Fund.

Bratspies, Rebecca M. 2018. "Cryptocurrency and the Myth of the Trustless Transaction."

Brenig, Christian, Rafael Accorsi, and Günter Müller. 2015. "Economic Analysis of Cryptocurrency Backed Money Laundering." ECIS.

Brewer, Russell, Melissa de Vel-Palumbo, Alice Hutchings, Thomas Holt, Andrew Goldsmith, and David Maimon. 2019. Cybercrime Prevention: Theory and Applications. Cham, Switzerland: Palgrave MacMillan.

Brito, Jerry 2014. "Benefits and Risks of Bitcoin for Small Businesses."

Broadhurst, Roderic. 2017. "Cybercrime in Australia." In *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, 221-235. Springer.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab, and Steve Chon. 2014. "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime." *International Journal of Cyber Criminology*: 1-20.

Broadhurst, Roderic, David Lord, Donald Maxim, Hannah Woodford-Smith, Corey Johnston, Ho Woon Chung, Samara Carroll, Harshit Trivedi, and Bianca Sabol. 2018. "Malware Trends on ‘Darknet’ crypto-Markets: Research Review."

Brooks, Graham 2012. "Online Gambling and Money Laundering: “Views from the Inside”." *Journal of Money Laundering Control* 15 (3): 304-315.

Broséus, Julian, Damien Rhumorbarbe, Marie Morelato, Ludovic Staehli, and Quentin Rossy. 2017. "A Geographical Analysis of Trafficking on a Popular Darknet Market." *Forensic science international* 277: 88-102.

Buchanan, Jim, and Alex J Grant. 2001. "Investigating and Prosecuting Nigerian Fraud." *US Attorney’s Bulletin* 49: 39.

Buchanan, William, Simon Dyson, and Liam Bell. 2018. "The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime." *The JBBA* 1 (2).

Budd, Christopher. 2016. "The State of Cyber Crime in the U.K." *Simply Security* (blog), *Trend Micro*. https://blog.trendmicro.com/the-state-of-cyber-crime-in-the-u-k/.

Burgess, Ann Wolbert, Meghan Mahoney, Julie Visk, and Leonard Morgenbesser. 2008. "Cyber Child Sexual Exploitation." *Journal of psychosocial nursing and mental health services* 46 (9): 38-45.

Burks, Christopher. 2017. "Bitcoin: Breaking Bad or Breaking Barriers?" *North Carolina Journal of Law Technology* 18 (5): 244.

Burns, Brett. 2011. "Level 85 Rogue: When Virtual Theft Merits Criminal Penalties." *UMKC L. Rev.* 80: 831.

Button, Mark, and Cassandra Cross. 2017. *Cyber Frauds, Scams and Their Victims*. Routledge.

Campbell-Verduyn, Malcolm. 2018. "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance." *Crime Law Social Change*: 1-23.

Canada Revenue Agency. 2019. *Guide for Cryptocurrency Users and Tax Professionals*. Ottawa: Government of Canada.

Canadian Centre for Cyber Security. 2018. *National Cyber Threat Assessment 2018*. Government of Canada.

Canadian Internet Registration Authority. 2018. *2018 Cira Canadian Internet Security Survey*. CIRA.

Cárdenas, Alvaro, Svetlana Radosavac, Jens Grossklags, John Chuang, and Chris Jay Hoofnagle. 2009. "An Economic Map of Cybercrime."

Carlisle, David, and Kayla Izenman. 2019. *Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia*. *Occasional Paper*. London: Royal United Services Institute for Defence and Security Studies.

Carmona, Anais. 2015. "The Bitcoin: The Currency of the Future, Fuel of Terror." In *Evolution of Cyber Technologies and Operations to 2035*, 127-135. Springer.

Carr, Angela. 2013. "The Social Dimension of the Online Trade of Child Sexual Exploitation Material." In *Understanding and Preventing Online Sexual Exploitation of Children*, 112-131. Routledge.

Carr, Madeline. 2016. "Public–Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92 (1): 43-62.

Carroll, Paul, and James Windle. 2018. "Cyber as an Enabler of Terrorism Financing, Now and in the Future." *Journal of Policing, Intelligence and Counter Terrorism* 13 (3): 285-300.

Carter, William A, and Daniel G Sofio. 2017. "Cybersecurity Legislation and Critical Infrastructure Vulnerabilities." In *Foundations of Homeland Security: Law and Policy*, 233-249. Wiley.

CASIS Vancouver. 2018. "Jackpotting and the Canadian Banking Environment." *The Journal of Intelligence, Conflict, and Warfare* 1 (2): 9-9.

Catota, Frankie E, M Granger Morgan, and Douglas C Sicker. 2019. "Cybersecurity Education in a Developing Nation: The Ecuadorian Environment." *Journal of Cybersecurity* 5 (1): tyz001.

Central Bank of Nigeria, February 28, 2018, "Virtual Currencies Not Legal Tender in Nigeria," https://www.cbn.gov.ng/out/2018/ccd/press%20release%20on%20virtual%20currencies.pdf.

Chainalysis. 2018. *The Changing Nature of Cryptocrime*. New York: Chainalysis.

---. 2019. *Crypto Crime Report: Decoding Increasingly Sophisticated Hacks, Darknet Markets, and Scams*. New York: Chainalysis.

Chaudhry, Peggy E. 2017. "The Looming Shadow of Illicit Trade on the Internet." *Business Horizons* 60 (1): 77-89.

Chawki, Mohamed. 2009. "Nigeria Tackles Advance Fee Fraud." *Journal of information, Law and Technology* 2009 (1).

Check Point. 2019. *Under the Hood of Cyber Crime: The Rise of Stealthy and Targeted Cyber Attacks*. 2019 Security Report Volume 02 ed. Tel Aviv: Check Point Software Technologies Ltd.

Chohan, Usman W. 2017. "Assessing the Differences in Bitcoin & Other Cryptocurrency Legality across National Jurisdictions." *Available at SSRN 3042248*.

Choi, Sinyong. 2018. "Illegal Gambling and Its Operation Via the Darknet and Bitcoin: An Application of Routine Activity Theory."

Christin, Nicolas. 2017. *An Eu-Focused Analysis of Drug Supply on the Online Anonymous Marketplace Ecosystem.* European Monitoring Centre for Drugs.

Chu, Bill, Thomas J Holt, and Gail Joon Ahn. 2012. Examining the Creation, Distribution, and Function of Malware On-Line. BiblioGov.

Chung, Wingyan, Hsinchun Chen, Weiping Chang, and Shihchieh Chou. 2006. "Fighting Cybercrime: A Review and the Taiwan Experience." *Decision Support Systems* 41 (3): 669-682.

Ciancaglini, Vincenzo, Marco Balduzzi, Max Goncharov, and Robert McArdle. 2013. *Deepweb and Cybercrime: It’s Not All About Tor*. Vol. 9. *Trend Micro Report*. Los Angeles: Trend Micro.

CipherTrace. 2019a. *Cryptocurrency Anti-Money Laundering Report, 2018 Q4*. CipherTrace.

---. 2019b. *Cryptocurrency Anti-Money Laundering Report, 2019 Q1*. CipherTrace.

Clapper, James R, Marcel Lettre, Admiral Michael S Rogers, USN Commander, and US Cyber Command. 2017. *Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States*.

Clark, Robert M, and Simon Hakim. 2016. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*. Vol. 3. Springer.

Clayton, Jay, 2017, "Statement on Cryptocurrencies and Initial Coin Offerings," https://web.archive.org/web/20190414102733/https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

"Coinmarketcap: Cryptocurrency Market Capitalizations." 2019. Accessed 29 October. https://web.archive.org/web/20191029215651/https://coinmarketcap.com/.

Conti, Mauro, Ankit Gangwal, and Sushmita Ruj. 2018. "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective." *Computers Security*.

Cooley, Alexander, John Heathershaw, and JC Sharman. 2018. "Laundering Cash, Whitewashing Reputations." *Journal of Democracy* 29 (1): 39-53.

Cooper, Sam. 2019. "Nearly $2 Billion in Dirty Money May Have Flowed through B.C. Casinos, Far More Than Official Estimates." *Global News*, 2019. https://web.archive.org/web/20190404104129/https://globalnews.ca/news/4897032/bc-casinos-money-laundering/.

Corbet, Shaen, Brian Lucey, Andrew Urquhart, and Larisa Yarovaya. 2018. "Cryptocurrencies as a Financial Asset: A Systematic Analysis." *International Review of Financial Analysis*.

Cotton, Jared. 2018. "Sending a Bit More Coin Home-an Analysis of Retail User Protection in Bitcoin Remittance Markets." *Victoria U. Wellington L. Rev.* 49: 107.

Crime in England and Wales: Additional Tables on Fraud and Cybercrime. 2019. edited by Office for National Statistics.

Cronin, Matthew 2018. "Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies." *US Attorney’s Bulletin.* 66: 65.

Cross, Cassandra. 2018. "Marginalized Voices: The Absence of Nigerian Scholars in Global Examinations of Online Fraud." In *The Palgrave Handbook of Criminology and the Global South*, 261-280. Springer.

Cunliffe, Jack, James Martin, David Décary-Hétu, and Judith Aldridge. 2017. "An Island Apart? Risks and Prices in the Australian Cryptomarket Drug Trade." *International Journal of Drug Policy* 50: 64-73.

Cusack, Brian, and Gerard Ward. 2018. "Points of Failure in the Ransomware Electronic Business Model."

Custers, Bart HM, Ronald LD Pool, and Remon Cornelisse. 2018. "Banking Malware and the Laundering of Its Profits." *European Journal of Criminology*: 1477370818788007.

De Groot, Juliana. 2019. "A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time." *Digital Guardian*.

de Koker, Louis. 2003. "Money Laundering Control: The South African Model." *Journal of Money Laundering Control* 6 (2): 166-181.

---. 2007. "Financial Crime in South Africa." *Economic Affairs* 27 (1): 34-38.

Décary-Hétu, David, Masarah Paquet-Clouston, and Judith Aldridge. 2016. "Going International? Risk Taking by Cryptomarket Drug Vendors." *International Journal of Drug Policy*.

Deibert, Ron. 2012. "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace." *Journal of military and strategic studies* 14 (2).

Deloitte. 2015. *Mitigating Emerging Fraud Risks in the Mobile Money Industry*. Deloitte Touche Tohmatsu India Private Limited.

Demant, Jakob, Silje Anderdal Bakken, Atte Oksanen, and Helgi Gunnlaugsson. 2019. "Drug Dealing on Facebook, Snapchat and Instagram: A Qualitative Analysis of Novel Drug Markets in the Nordic Countries." *Drug and alcohol review* 38 (4): 377-385.

Department of Economic Affairs: Ministry of Finance. 2019. *Report of the Committee to Propose Specific Actions to Be Taken in Relation to Virtual Currencies*. New Delhi: Department of Economic Affairs: Ministry of Finance.

Department of Foreign Affairs and Trade. 2017. *Australia’s International Cyber Engagement Strategy*. Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade.

Department of Telecommunications and Postal Services. 2017. *Cybersecurity Readiness Report 2017*. Pretoria: Department of Telecommunications and Postal Services.

Desjardins, Jeff. 2017. "All of the World’s Money and Markets in One Visualization." The Money Project. Visual Capitalist. Accessed 13 October. https://web.archive.org/web/20191013094827/https://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/.

Digital Shadows Photon Research Team. 2019. *A Tale of Epic Extortions How Cybercriminals Monetize Our Online Exposure*. London: Digital Shadows.

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. 2019. *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. Santa Monica, CA: RAND Corporation.

Dittrich, David. 2012. "So You Want to Take over a Botnet." The 5th USENIX conference on Large-Scale Exploits and Emergent Threats, San Jose, California.

Don, M, Nicholas Clarke, and Danling Jiang. 2019. "Bitcoin Speculation or Value Creation? Corporate Blockchain Investments and Stock Market Reactions." *Corporate Blockchain Investments and Stock Market Reactions (May 1, 2019)*.

Dubey, Rajiv. 2018. "More Cash in Market Now Than before Demonetisation Day, RBI Data Shows." *India Today*, November 8, 2018. https://web.archive.org/web/20190330133534/https://www.indiatoday.in/india/story/demonetisation-more-cash-rbi-data-1384452-2018-11-08.

Ducas, Evangeline, and Alex Wilner. 2017. "The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada." *International Journal* 72 (4): 538-562.

Dupont, Benoît. 2016. "Les Liens Faibles Du Crime En Ligne: Écologie De La Méfiance Au Sein De Deux Communautés De Hackers Malveillants." 3 (1): 109-136.

Edwards, Adam. 2016. "Actors, Scripts, Scenes and Scenarios: Key Trends in Policy and Research on the Organisation of Serious Crimes."

Egan, Mo. 2018. "A Bit (Coin) of a Problem for the EU AML Framework." In *The Palgrave Handbook of Criminal and Terrorism Financing Law*, 183-208. Springer.

Elendner, Hermann, Simon Trimborn, Bobby Ong, and Teik Ming Lee. 2018. "The Cross-Section of Crypto-Currencies as Financial Assets: Investing in Crypto-Currencies Beyond Bitcoin." In *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1*, 145-173. Elsevier.

Elliptic, 2019, "Consultation on 5amld."

Eoyang, Mieke, Allison Peters, Ishan Mehta, and Brandon Gaskew. 2018. *To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors*. Washington D.C.: Third Way.

ESAAMLG. 2018. *First Round Mutual Evaluations - Post Evaluation Progress Report of South Africa*. ESAAMLG.

Etaher, Najla, George RS Weir, and Mamoun Alazab. 2015. "From Zeus to Zitmo: Trends in Banking Malware." 2015 IEEE Trustcom/BigDataSE/ISPA.

European Central Bank. 2012. *Virtual Currency Schemes*. Frankfurt am Main: European Central Bank.

Europol. 2013. *Cyberbits.* Europol (The Hague: Europol).

---. 2015. *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European Union Agency for Law Enforcement Cooperation.

---. 2018. *The Internet Organised Crime Threat Assessment (IOCTA)*. The Hague: European Union Agency for Law Enforcement Cooperation.

Fanusie, Yaya, and Tom Robinson. 2018. "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services."

FATF. October 18, 2013. *Improving Global AML/CFT Compliance: On-Going Process, 18 October 2013.* FATF (Paris).

---. 2016a. *Anti-Money Laundering and Counter-Terrorist Financing Measures, Canada, Mutual Evaluation Report*. Paris: FATF and APG.

---. 2016b. *Anti-Money Laundering and Counter-Terrorist Financing Measures, United States, Mutual Evaluation Report*. Paris: FATF and APG.

---. 2018a. *8th Follow-up Report: Mutual Evaluation of India.* FATF (Paris).

---. 2018b. *Anti-Money Laundering and Counter-Terrorist Financing Measures, United Kingdom, Mutual Evaluation Report*. Paris: FATF.

---. October 18 2018c. *Anti-Money Laundering and Counter-Terrorist Financing Measures: Australia.* FATF (Paris).

---. October 18 2018d. *FATF Report to the G20 Finance Ministers and Central Bank Governors.* FATF (Paris).

---. 2019. "Improving Global AML/CFT Compliance: On-Going Process - 21 June 2019." FATF. Accessed 7 November. https://web.archive.org/web/20191107170301/https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/fatf-compliance-june-2019.html.

FBI. 2014. *2014 Internet Crime Report*. Internet Crime Complaint Center.

---. 2017. *2016 Internet Crime Report.* Federal Bureau of Investigation.

---. 2018. *2017 Internet Crime Report.* Federal Bureau of Investigation.

Federal Reserve Board. 2018. *Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study*. Washington D.C.: Federal Reserve Board.

Fein, Melanie L. 2018. "Bitcoin: How Is It Regulated?".

Felson, Marcus, and Ronald V Clarke. 1998. "Opportunity Makes the Thief." *Police research series, paper* 98.

Fiedler, Ingo. 2013. "Online Gambling as a Game Changer to Money Laundering?" *Available at SSRN 2261266*.

Financial Conduct Authority. 2018. *Financial Crime: Analysis of Firms' Data*. London: Financial Conduct Authority.

Financial Intelligence Centre. 2018a. *Annual Report*. Centurion, South Africa: Financial Intelligence Centre.

---. 2018b. *Scams and Typologies*. Centurion, South Africa: Financial Intelligence Centre.

---. 2018c. *Typologies*. Centurion, South Africa: Financial Intelligence Centre.

Financial Intelligence Unit-India. 2018. *Annual Report 2017-18*. Financial Intelligence Unit-India, Department of Revenue, Ministry of Finance, Government of India.

FINTRAC. 2018. *Fintrac Annual Report 2017-18*. Ottawa: Financial Transactions and Reports Analysis Centre of Canada.

Flashpoint. 2016. *2015 Highlights & Trends in the Deep and Dark Web*. Flashpoint.

Forgang, George. 2019. "Money Laundering through Cryptocurrencies."

FTR Team. 2015. *U-Markt: Peering into the German Cybercriminal Underground*. *Trendlabs Research Paper*. Los Angeles: Trend Micro.

FTR Team, and European Cybercrime Centre. 2017. *Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types*. Los Angeles: TrendMicro.

Fuentes, Mayra Rosario. 2017. *Digital Souks: A Glimpse into the Middle Eastern and North African Underground*. Los Angeles: Trend Micro, Incorporated.

Gainsbury, Sally M, and Alex Blaszczynski. 2017. "How Blockchain and Cryptocurrency Technology Could Revolutionize Online Gambling." *Gaming Law Review* 21 (7): 482-492.

Galdo, Michael C, Monica E Tait, and Lisa Feldman. 2018. "Money Mules: Stopping Older Adults and Others from Participating in International Crime Schemes." *US Attorney's Bulletin* 66: 95.

Gallagher, Harold, Wade McMahon, and Ron Morrow. 2014. "Cyber Security: Protecting the Resilience of Canada's Financial System." *Bank of Canada Financial System Review*: 47-53.

Gandal, Neil, JT Hamrick, Tyler Moore, and Tali Oberman. 2018. "Price Manipulation in the Bitcoin Ecosystem." *Journal of Monetary Economics* 95: 86-96.

Garg, Preeti, and Manvi Panchal. 2016. "Study on Introduction of Cashless Economy in India 2016: Benefits & Challenge's." *Journal of Business and Management* 19 (4): 116-120.

Gaspareniene, Ligita, and Rita Remeikiene. 2015. "Digital Shadow Economy: A Critical Review of the Literature." *Mediterranean Journal of Social Sciences* 6 (6 S5): 402.

Gault, Matthew. 2019. "Nearly All' Counter-Strike Microtransactions Are Being Used for Money Laundering." *Vice*.

Gautam, Apurv Singh, Yamini Gahlot, and Pooja Kamat. 2019. "Hacker Forum Exploit and Classification for Proactive Cyber Threat Intelligence." International Conference on Inventive Computation Technologies.

Gendron, Angela, and Martin Rudner. 2012. *Assessing Cyber Threats to Canadian Infrastructure*. The Canadian Security Intelligence Service.

German, Peter. 2018. *Dirty Money: An Independent Review of Money Laundering in Lower Mainland Casinos Conducted for the Attorney General of British Columbia*. Vancouver: Government of British Columbia.

Ghernaouti-Hélie, Solange. 2012. "The Cybercrime Ecosystem & Privacy Issues Main Challenges and Perspectives from a Societal Perspective." *Cybercrime*: 10.

Ghosh, Shalini, Phillip Porras, Vinod Yegneswaran, Ken Nitz, and Ariyam Das. 2017. "ATOL: A Framework for Automated Analysis and Categorization of the Darkweb Ecosystem." Workshops at the Thirty-First AAAI Conference on Artificial Intelligence.

GIABA. 2015. *Seventh Follow up Report: Mutual Evaluation, Nigeria*. Ponty Dakar, Senegal: GIABA.

Girasa, Rosario. 2018. "States’ Regulation of Virtual Currencies." In *Regulation of Cryptocurrencies and Blockchain Technologies*, 115-137. Springer.

Glaser, Florian, Kai Zimmermann, Martin Haferkorn, Moritz Christian Weber, and Michael Siering. 2014. "Bitcoin-Asset or Currency? Revealing Users' Hidden Intentions."

Godse, Vinayak. 2016. *Building an Ecosystem for Cyber Security and Data Protection in India*. New Delhi.

Goncharov, Max. 2015. Criminal Hideouts for Lease: Bulletproof Hosting Services. Trend Micro.

Goodman, Marc. 2011. "International Dimensions of Cybercrime." In *Cybercrimes: A Multidisciplinary Analysis*, edited by Sumit Ghosh and Elliot Turrini, 311-339. Berlin, Heidelberg: Springer Berlin Heidelberg.

Government of Canada. 2019. "Regulations Amending Certain Regulations Made under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019: Sor/2019-240." *Canada Gazette* 153, no. II (14). http://www.gazette.gc.ca/rp-pr/p2/2019/2019-07-10/html/sor-dors240-eng.html.

Gu, Lion. 2014. *The Mobile Cybercriminal Underground Market in China*. *Cybercriminal Underground Economy Series*. Irving, Texas: Trend Micro.

Guerrero-Saade, Juan Andres, and Priscilla Moriuchi. 2018. "North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign." *Recorded Future* 16.

Gundur, R.V. 2019. "Finding the Sweet Spot: Optimizing Criminal Careers within the Context of Illicit Enterprise." *Deviant Behavior*. https://doi.org/10.1080/01639625.2019.1565851.

Guri, Mordechai 2018. "Beatcoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets."

Halder, Debarati, and K Jaishankar. 2016. *Cyber Crimes against Women in India*. SAGE Publications India.

Head, Tom. 2019. "City of Joburg Held to Ransom: Hackers Threaten to Release Personal Data." *The South African*, 2019. https://web.archive.org/web/20191106225309/https://www.thesouthafrican.com/tech/city-of-joburg-hackers-what-is-ransom-bitcoins-worth-who-affected/.

Hennessey, Susan. 2017. "Deterring Cyberattacks: How to Reduce Vulnerability." *Foreign Affairs.* 96: 39.

Hernandez, Sandra Concepcion Layla S, Andrew C Lacsina, Michelle C Ylade, Josephine Aldaba, Hilton Y Lam, Leonardo R Estacio Jr, and Anna Lena Lopez. 2018. "Sexual Exploitation and Abuse of Children Online in the Philippines: A Review of Online News and Articles." *Acta Medica Philippina* 52 (4): 306.

Hileman, Garrick, and Michel Rauchs. 2017. "Global Cryptocurrency Benchmarking Study." *Cambridge Centre for Alternative Finance* 33.

HM Government. 2016. *National Cyber Security Strategy 2016-2021.* HM Government (London).

HM Treasury. 2019. *Transposition of the Fifth Money Laundering Directive: Consultation*. London: Crown.

HMICFRS. 2019a. *Cyber: Keep the Light on an Inspection of the Police Response to Cyber-Dependent Crime*. London: Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services.

---. 2019b. *Fraud: Time to Choose: An Inspection of the Police Response to Fraud*. London: Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services.

HO News Team, 2017, "Economic Crime Factsheet," https://web.archive.org/web/20190415092612/https://homeofficemedia.blog.gov.uk/2017/12/11/economic-crime-factsheet/.

Hooper, Christopher, Ben Martini, and Kim-Kwang Raymond Choo. 2013. "Cloud Computing and Its Implications for Cybercrime Investigations in Australia." *Computer Law & Security Review* 29 (2): 152-163.

House of Commons Treasury Committee. 2018. *Crypto-Assets*. London: House of Commons.

Hutchings, Alice. 2018. "Leaving on a Jet Plane: The Trade in Fraudulently Obtained Airline Tickets." *Crime Law Social Change* 70 (4): 461-487.

Hutchings, Alice, and Thomas J. Holt. 2015. "A Crime Script Analysis of the Online Stolen Data Market." *British Journal of Criminology* 55 (3): 596-614. https://doi.org/10.1093/bjc/azu106.

Hutchings, Alice, and Sergio Pastrana. 2019. "Understanding eWhoring." *arXiv preprint arXiv:1905.04576*.

Ianelli, Nicholas, and Aaron Hackworth. 2005. "Botnets as a Vehicle for Online Crime." *The International Journal of Forensic Computer Science* 2 (1): 19-39.

Ibragimove, T, O Kupreev, E Badovskaya, and A Gutnikov. 2018. "Ddos Attacks in Q2 2018." Securelist.

Ibrahim, Suleman. 2016. "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals." *International Journal of Law, Crime and Justice* 47: 44-57.

International Telecommunications Union. 2019. "Internet Users by Region and Country, 2010-2016." International Telecommunications Union. Accessed March 24. https://web.archive.org/save/https://www.itu.int/en/ITU-D/Statistics/Pages/stat/Treemap.aspx.

INTERPOL. 2018a. *Annual Report 2017*. Lyon: INTERPOL.

---. 2018b. *Global Cybercrime Strategy*. Lyon: INTERPOL.

---. 2018c. *Overview of Serious and Organized Crime in Africa*. Lyon: INTERPOL General Secretariat.

---. 2018d. *Overview of Serious and Organized Crime in Central Africa*. Lyon: INTERPOL General Secretariat.

---. 2018e. *Overview of Serious and Organized Crime in East Africa*. Lyon: INTERPOL General Secretariat.

---. 2018f. *Overview of Serious and Organized Crime in North Africa*. Lyon: INTERPOL General Secretariat.

---. 2018g. *Overview of Serious and Organized Crime in the Southern African Region*. Lyon: INTERPOL General Secretariat.

---. 2018h. *Overview of Serious and Organized Crime in West Africa*. Lyon: INTERPOL General Secretariat.

Iqbal, Juneed, and Bilal Maqbool Beigh. 2017. "Ethical Aspects of Software Engineering: A Wake up Call for India." *vol* 5: 53-62.

Irons, Alastair, and Jacques Ophoff. 2016. "Aspects of Digital Forensics in South Africa." *Interdisciplinary Journal of Information, Knowledge, and Management* 11: 273-283.

Irwin, Angela SM, and Caitlin Dawson. 2019. "Following the Cyber Money Trail: Global Challenges When Investigating Ransomware Attacks and How Regulation Can Help." *Journal of Money Laundering Control*.

Irwin, Angela SM, and Adam B Turner. 2018. "Illicit Bitcoin Transactions: Challenges in Getting to the Who, What, When and Where." *Journal of Money Laundering Control* 21 (3): 297-313.

Jakobi, Anja P. 2018. "Governing Illicit Finance in Transnational Security Spaces: The FATF and Anti-Money Laundering." *Crime, Law and Social Change* 69 (2): 173-190.

Janze, Christian. 2017. "Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets."

Jianwei, Zhuge, Gu Liang, and Duan Haixin. 2012. "Investigating China’s Online Underground Economy." Conference on the Political Economy of Information Security in China.

Johan Lor, Peter, and Johannes Britz. 2005. "Knowledge Production from an African Perspective: International Information Flows and Intellectual Property⋆." *The International Information & Library Review* 37 (2): 61-76.

Johnson, Kristin N. 2015a. "Cyber Risks: Emerging Risk Management Concerns for Financial Institutions." *Ga. L. Rev.* 50: 131.

Johnson, Thomas A. 2015b. *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. CRC Press.

Jost, Patrick M, and Harjit Singh Sandhu. 2003. *The Hawala Alternative Remittance System and Its Role in Money Laundering*. Lyon, France: Interpol.

Kandpal, Vineet, and RK Singh. 2013. "Latest Face of Cybercrime and Its Prevention in India." *International Journal of Basic and Applied Sciences* 2 (4): 150-156.

Kappos, George, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. 2018. "An Empirical Analysis of Anonymity in Zcash." 27th {USENIX} Security Symposium ({USENIX} Security 18).

Katsuki, Takeo, Tim Ken Mackey, and Raphael Cuomo. 2015. "Establishing a Link between Prescription Drug Abuse and Illicit Online Pharmacies: Analysis of Twitter Data." *Journal of medical Internet research* 17 (12).

Kazeem, Yomi. 2018. "Nigeria’s Central Bank Could Hamstring Local Fintech Startups with Costly New Regulation." *Quartz Africa*, 2018.

Kim, S Thomas. 2019. "Bitcoin Dilemma: Is Popularity Destroying Value?" *Finance Research Letters*.

Kleijssen, Jan, and Pierluigi Perri. 2017. "Cybercrime, Evidence and Territoriality: Issues and Options." In *Netherlands Yearbook of International Law 2016*, 147-173.

Springer.

KPMG. 2017. *Cybercrime Survey Report*. India: KPMG.

Kshetri, Nir. 2010. "Diffusion and Effects of Cyber-Crime in Developing Economies." *Third World Quarterly* 31 (7): 1057-1079.

---. 2013. *Cybercrime and Cybersecurity in the Global South*. Springer.

---. 2015. "Cybercrime and Cybersecurity Issues in the BRICS Economies." *Journal of Global Information Technology Management* 18 (4): 245-249.

---. 2016. "Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future." *Crime, Law and Social Change* 66 (3): 313-338.

---. 2017. "Cybersecurity in India: Regulations, Governance, Institutional Capacity and Market Mechanisms." *Asian Research Policy* 8 (1): 64-76.

Kujawa, Adam, Wendy Zamora, Jovi Umawing, Jerome Segura, William Tsing, Adam McNeil, Pieter Arntz, and Chris Boyd. 2018. *Cybercrime Tactics and Techniques: Q3 2018*. Malwarebytes Labs.

Laszka, Aron, Benjamin Johnson, Pascal Schöttle, Jens Grossklags, and Rainer Böhme. 2014. "Secure Team Composition to Thwart Insider Threats and Cyber-Espionage." *ACM Transactions on Internet Technology (TOIT)* 14 (2-3): 19.

Lee, Joseph. 2019. "'We Lost Nearly £10k to Tv Licence Scammers'." *BBC News*, 2019. https://web.archive.org/web/20190414130413/https://www.bbc.com/news/uk-46765681.

Leukfeldt, Rutger. 2014. "Cybercrime and Social Ties." *Trends in Organized Crime* 17 (4): 231-249.

Leukfeldt, Rutger, and Jurjen Jansen. 2015. "Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands." *International Journal of Cyber Criminology* 9 (2): 173.

Leukfeldt, Rutger, Edward Kleemans, and Wouter Stol. 2017. "The Use of Online Crime Markets by Cybercriminal Networks: A View from Within." *American Behavioral Scientist* 61 (11): 1387-1402.

Levi, Michael. 2013. "E-Gaming, Money Laundering and the Problem of Risk Assessment." In *Research Handbook on Money Laundering*, edited by Brigitte Unger and Daan van der Linde, 332. Cheltanham: Edward Elgar.

---. 2015. "Foreword: Some Reflections on the Evolution of Economic and Financial Crimes." In *Research Handbook on International Financial Crime*. Edward Elgar Publishing.

---. 2020. “Evaluating the Control of Money Laundering and Its Underlying Offences: The Search for Meaningful Data”, *Asian Journal of Criminology*¸ 1-20.

Levi, Michael, Peter Reuter, and Terrence Halliday. “Can the AML/CTF System Be Evaluated Without Better Data?” *Crime, Law and Social Change*, 69(2), 307-328.

Levi, Michael, and Melvin R J Soudijn. 2020. "Understanding the Laundering of Organized Crime Money." In Peter Reuter and Michael Tonry (eds.) Organizing Crime: Mafias, Markets, and Networks, *Crime and Justice: An Annual Review of Research*, 49: 579-631

Libra Association Members. 2019. *An Introduction to Libra*. Geneva: The Libra Association.

Lindsay, Jon R, Tai Ming Cheung, and Derek S Reveron. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, USA.

Lo, William Yat Wai. 2011. "Soft Power, University Rankings and Knowledge Production: Distinctions between Hegemony and Self-Determination in Higher Education." *Comparative Education* 47 (2): 209-222.

Lubold, Gordon, and Dustin Volz. 2019. "Navy, Industry Partners Are ‘under Cyber Siege’ by Chinese Hackers, Review Asserts." *Wall Street Journal*, 2019. https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553?mod=article_inline.

Lusthaus, Jonathan, and Federico Varese. 2017. "Offline and Local: The Hidden Face of Cybercrime." *Policing: A Journal of Policy and Practice*.

Lycka, Martin 2011. "Online Gambling: Towards a Transnational Regulation." *Gaming Law Review* 15 (4): 179-195.

Mackey, Tim K, and Bryan A Liang. 2011. "The Global Counterfeit Drug Trade: Patient Safety and Public Health Risks." *Journal of pharmaceutical sciences* 100 (11): 4571-

4579.

MacRae, John, and Virginia NL Franqueira. 2017. "On Locky Ransomware, Al Capone and Brexit." International Conference on Digital Forensics and Cyber Crime.

Mahdavieh, Rose. 2019. "Governments' Adoption of Native Cryptocurrency: A Case Study of Iran, Russia, and Venezuela."

Mandiant. 2016. *M-Trends 2016: A View from the Front Lines*. Fireeye.

---. 2017. *M-Trends 2017: A View from the Front Lines*. FireEye.

Manky, Derek. 2013. "Cybercrime as a Service: A Very Modern Business." *Computer Fraud Security* 2013 (6): 9-13.

Mansfield-Devine, Steve. 2015. "The Growth and Evolution of Ddos." *Network Security* 2015 (10): 13-20. https://doi.org/10.1016/s1353-4858(15)30092-1.

---. 2016. "The Imitation Game: How Business Email Compromise Scams Are Robbing Organisations." *Computer Fraud & Security* 2016 (11): 5-10.

Marria, Vishal. 2018. "What a Cashless Society Could Mean for the Future." *Forbes*.

Matsakis, Louise. 2018. "The Us Sits out an International Cybersecurity Agreement." *Wired*.

Maurushat, Alana. 2010. "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools." *UNSWLJ* 33: 431.

Mbelli, Thierry Mbah, and Barry Dwolatzky. 2016. "Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security." 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud).

McCartney, Edward. 2017. "Nested Payment Intermediaries in the Ach Network: Risks and Responsibilities of ODFIs." *NC Banking Inst.* 21: 405.

McFarland, Charles, Francois Paget, and Raj Samani. 2015. "The Hidden Data Economy. The Marketplace for Stolen Digital Information." *Intel Security*: 20151015-01.

McGinn, Dan, David Birch, David Akroyd, Miguel Molina-Solana, Yike Guo, and William Knottenbelt. 2016. "Visualizing Dynamic Bitcoin Transaction Patterns." *Big Data* 4 (2):

109-119.

McGuire, Michael. 2018. *Into the Web of Profit.* Bromium.

McMullan, John L, and Aunshul Rege. 2010. "Online Crime and Internet Gambling." *Journal of Gambling Issues* (24): 54-85.

Meissner, Dirk. 2019. "Money Laundering in B.C. Estimated at $1b a Year — but Reports Were Not Shared with Province, Ag Says." *CBC*, 2019. https://web.archive.org/web/20190406115336/https://www.cbc.ca/news/canada/british-columbia/money-laundering-billions-bc-david-eby-1.4983471.

Merdian, Hannah Lena, Cate Curtis, Jo Thakker, Nick Wilson, and Douglas Pieter Boer. 2013. "The Three Dimensions of Online Child Pornography Offending." *Journal of sexual aggression* 19 (1): 121-132.

Mikhaylov, Alexander, and Richard Frank. 2016. "Cards, Money and Two Hacking Forums: An Analysis of Online Money Laundering Schemes." 2016 European Intelligence and Security Informatics Conference (EISIC).

Ministry of Home Affairs. 2019. "Cybercrime Reporting Portal." https://web.archive.org/web/20190330082551/https://cybercrime.gov.in/cybercitizen/home.htm.

Moens, Alexander, Seychelle Cushing, and Alan W Dowd. 2015. *Cybersecurity Challenges for Canada and the United States*. Fraser Institute.

Mohammed, Kabiru H, Yusuf D Mohammed, and Abiodun A Solanke. 2019. "Cybercrime and Digital Forensics: Bridging the Gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria." *International Journal of Cybersecurity Intelligence & Cybercrime* 2 (1): 56-63.

Moiseienko, Anton, and Kayla Izenman. 2019. *Gaming the System: Money Laundering through Online Games*. London: Royal United Services Institute for Defence and Security Studies.

Moiseienko, Anton, and Olivier Kraft. 2018. *From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime*. London: Royal United Services Institute for Defence and Security Studies.

Moiseienko, Anton, and Tom Keatinge. 2019. The Scale of Money Laundering in the UK: Too Big to Measure? London: Royal United Services Institute for Defence and Security Studies.

Mullan, P Carl. 2016. *History of Digital Currency in the United States*. Springer.

Nappinai, NS. 2010. "Cyber Crime Law in India: Has Law Kept Pace with Engineering Trends-an Empirical Study." *J. Int'l Com. L. & Tech.* 5: 22.

Narayan, Shannu. 2018. "Anti-Money Laundering Law in India: A 'Glocalization' model." *Statute Law Review*.

National Bureau of Statistics. 2018. *Labor Force Statistics - Volume I: Unemployment and Underemployment Report*. Abuja: National Bureau of Statistics.

National Crime Records Bureau. 2017. *Crime in India 2016*. New Delhi: Ministry of Home Affairs, Government of India.

NCA. 2020. National Strategic Assessment of Serious and Organised Crime. London: National Crime Agency.

O'Brien, Dick. 2017. *Istr Ransomware 2017*. Symantec.

Obuah, Emmanuel. 2010. "Combatting Corruption in Nigeria: The Nigerian Economic and Financial Crimes (EFCC)." *African Studies Quarterly* 12 (1): 17-45.

Ogunbadewa, Ajibola. 2013. "The Bitcoin Virtual Currency: A Safe Haven for Money Launderers?".

---. 2014. "The Virtues and Risks Inherent in the 'Bitcoin' Virtual Currency."

Ogwezzy, Michael Chukwujindu. 2012. "Cyber Crime and the Proliferation of Yahoo Addicts in Nigeria." *AGORA Int'l J. Jurid. Sci.*: 86.

Okeshola, Folashade B, and Abimbola K Adeta. 2013. "The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria." *American International Journal of Contemporary Research* 3 (9): 98-114.

Oleksiewicz, Izabela. 2019. "Policy to Prevent and Combat Cyber-Crime in Africa." *Humanities and Social Sciences* 7 (4): 138.

Omeire, Edward, and Charles Omeire. 2016. "Social Structure and the Production of Young Cyber Criminals in Nigeria."

Omodunbi, BA, PO Odiase, OM Olaniyan, and AO Esan. 2016. "Cybercrimes in Nigeria: Analysis, Detection and Prevention." *Journal of Engineering and Technology* 1 (1): 37-42.

Ontario Securities Commission. 2018. *Taking Caution: Financial Consumers and the Cryptoasset Sector*. Toronto: Ontario Securities Commission.

Orsolini, Laura, Giulia Francesconi, Duccio Papanti, Arianna Giorgetti, and Fabrizio Schifano. 2015. "Profiling Online Recreational/Prescription Drugs' Customers and Overview of Drug Vending Virtual Marketplaces." *Human Psychopharmacology: Clinical and Experimental* 30 (4): 302-318.

Oyebayo, Damilola A., and Rilwan Shittu. 2018. "Evaluating the Central Bank of Nigeria's Directive on Cryptocurrency." *Nigerian Law Today* (blog). 28 October. https://web.archive.org/save/http://nigerianlawtoday.com/evaluating-central-bank-nigerias-directive-cryptocurrency/.

Pace, Jonathan. 2017. "Exchange Relations on the Dark Web." *Critical Studies in Media Communication* 34 (1): 1-13.

Paquet-Clouston, Masarah, Bernhard Haslhofer, and Benoit Dupont. 2019. "Ransomware Payments in the Bitcoin Ecosystem." *Journal of Cybersecurity* 5 (1): tyz003.

Pasti, Francesco. 2019. *State of the Industry Report on Mobile Money: 2018*. London: GSM Association.

Pastrana, Sergio, and Guillermo Suarez-Tangil. 2019. "A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth."

Patterson, Nicholas C, and Michael Hobbs. 2010. "A Multidiscipline Approach to Governing Virtual Property Theft in Virtual Worlds." In *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience*, 161-171. Springer.

Paul, Kari. 2019. "Payment Firms Back out in Painful Blow to Facebook's Cryptocurrency Libra." *The Guardian*, 2019. https://web.archive.org/web/20191030225126/https://www.theguardian.com/technology/2019/oct/11/payment-firms-back-out-in-painful-blow-to-facebooks-cryptocurrency-libra.

Pernet, Cedric. 2016. *The French Underground: Under a Shroud of Extreme Caution.* Trend Micro (Trend Micro). https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-french-underground-under-a-shroud-of-extreme-caution.

Pomemon Institute. 2017. *Cost of Cyber Crime Study*. Accenture.

Ponemon Institute. 2019. *The Cost of Cybercrime*. Traverse City, Michigan: Accenture.

Poon, Joseph, and Thaddeus Dryja. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.

Public Safety Canada. 2018. *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Her Majesty the Queen in Right of Canada.

Putong, Diana Darmayanti, Quido Conferti Kainde, and Pudji Astuti. 2018. "Money Laundering in the It Era." 1st International Conference on Social Sciences (ICSS 2018).

PwC. 2018a. *Pulling Fraud out of the Shadows: 2018 Global Economic Crime and Fraud Survey: UK Findings*. PricewaterhouseCooper.

---, 2018b, "Reported Economic Crime in South Africa Hits Record Levels," https://web.archive.org/web/*/https://www.pwc.co.za/en/press-room/reported-economic-crime-in-south-africa-hits-record-levels.html.

Rana, Marthe, 2018, "Developer Population Growth Shifts toward China, India and Emerging Countries," https://web.archive.org/save/https://evansdata.com/press/viewRelease.php?pressID=268.

Reaves, Bradley, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin RB Butler. 2017. "Mo(Bile) Money, Mo(Bile) Problems." *ACM Transactions on Privacy and Security* 20 (3): 1-31.

Reinhart, RJ, 2018, "One in Four Americans Have Experienced Cybercrime," https://web.archive.org/web/20190413070939/https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx.

Remorin, Lord, Ryan Flores, and Bakuei Matsukawa. 2018. *Tracking Trends in Business Email Compromise (Bec) Schemes.* Technical report, Trend Micro.

Reserve Bank of India, 2018, "Statement on Developmental and Regulatory Policies."

Richet, Jean-Loup. 2013. "Laundering Money Online: A Review of Cybercriminals Methods." *arXiv preprint arXiv:1310.2368*.

Rueckert, Christian. 2019. "Cryptocurrencies and Fundamental Rights." *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyz004.

Runde, Daniel. 2015. "M-Pesa and the Rise of the Global Mobile Money Market." *Forbes*.

Rusch, Jonathan J. 1999. "The “Social Engineering” of Internet Fraud." Internet Society Annual Conference, San Jose, CA.

Salvi, Harshada U, and Ravindra V Kerkar. 2016. "Ransomware: A Cyber Extortion." *Asian Journal of Convergence in Technology* 2.

Samani, Raj, and Charles McFarland. 2015. *Hacking the Human Operating System the Role of Social Engineering within Cybersecurity.* McAfee (Santa Clara, CA).

Samani, Raj, François Paget, and Matthew Hart. 2013. *Digital Laundry: An Analysis of Online Currencies, and Their Use in Cybercrime*. Santa Clara, CA: McAfee.

Samtani, Sagar, Ryan Chinn, Hsinchun Chen, and Jay F. Nunamaker. 2018. "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence." *Journal of Management Information Systems* 34 (4): 1023-1053. https://doi.org/10.1080/07421222.2017.1394049.

Sanni, Serah Onyeche. 2019. "Nigeria: Crypto Currency in Nigeria: Regulatory Framework & Related Issues." *Mondaq* (blog), *Mondaq*. https://web.archive.org/web/20191022190424/http://www.mondaq.com/Nigeria/x/855410/fin+tech/Crypto+Currency+In+Nigeria+Regulatory+Framework+Related+Issues.

Saunders, Jamie. 2017. "Tackling Cybercrime–the UK Response." *Journal of Cyber Policy* 2 (1): 4-15.

SecureWorks. 2016. *Underground Hacker Markets: Annual Report 2016*. Dell SecureWorks.

Segrave, Marie, and Laura Vitis. 2017. *Gender, Technology and Violence*. Routledge.

Selmi, Refk, Aviral Kumar Tiwari, and Shawkat Hammoudeh. 2018. "Efficiency or Speculation? A Dynamic Analysis of the Bitcoin Market." *Economics Bulletin* 38 (4): 2037-2046.

Seok, Soonhwa, and Boaventura DaCosta. 2019. "The Cyber Awareness of Online Video Game Players: An Examination of Their Online Safety Practices and Exposure to Threats." *International Journal of Cyber Research and Education (IJCRE)* 1 (1): 69-77.

Shakarian, Jana, Andrew T Gunn, and Paulo Shakarian. 2016. "Exploring Malicious Hacker Forums." In *Cyber Deception*, 259-282. Springer.

Shakarian, Paulo, and Jana Shakarian. 2016. "Socio-Cultural Modeling for Cyber Threat Actors." Workshops at the Thirtieth AAAI Conference on Artificial Intelligence.

Shanaev, Savva, Satish Sharma, Binam Ghimire, and Arina Shuraeva. 2020. "Taming the Blockchain Beast? Regulatory Implications for the Cryptocurrency Market." *Research in International Business and Finance* 51: 101080.

Shehu, Abdullahi Y. 2004. "The Asian Alternative Remittance Systems and Money Laundering." *Journal of Money Laundering Control* 7 (2): 175-185.

Sheth, Arpan, Joydeep Bhattacharya, Amit Shah, Rajan Anandan, Vikas Agnihotri, Pankaj Gupta, Raman Chadha, Roopa Kudva, Siddharth Nautiyal, and Sushant Kumar. 2018. *Unlocking Digital for Bharat $50 Billion Opportunity*. Bain & Company, Google India, and Omidyar Network.

Shirley, M Angel Jasmine. 2017. "Impact of Demonetization in India." *International Journal of Trend in Research and Development*: 20-23.

Sicetsha, Andile. 2018. "Saps Cybercrime Unit Unable to Function Due to Expired Software Licenses." *The South African*, 2018. https://web.archive.org/web/20190403133740/https://www.thesouthafrican.com/saps-cybercrime-unit-expired-software-license/.

Sigler, Karl 2018. "Crypto-Jacking: How Cyber-Criminals Are Exploiting the Crypto-Currency Boom." *Computer Fraud Security* 2018 (9): 12-14.

Sirila, Diana. 2014. "The Pleasures and Perils of New Money in Old Pockets; M-Pesa and Bitcoin in Kenya."

Slayton, T. B. 2018. "Ransomware: The Virus Attacking the Healthcare Industry." *J Leg Med* 38 (2): 287-311. https://doi.org/10.1080/01947648.2018.1473186. https://www.ncbi.nlm.nih.gov/pubmed/30289741.

Smirnova, Olga, and Thomas Holt. 2017. "Examining the Geographic Distribution of Victim Nations in Stolen Data Markets." *American Behavioral Scientist* 61 (11): 1403-1426.

Sotiropoulou, Anastasia, and Dominique Guégan. 2017. "Bitcoin and the Challenges for Financial Regulation." *Capital Markets Law Journal* 12 (4): 466-479.

South African Reserve Bank. 2014. *Position Paper on Virtual Currencies*. Pretoria: South African Reserve Bank.

Speer, David L. 2000. "Redefining Borders: The Challenges of Cybercrime." *Crime, Law and Social Change* 34 (3): 259-273. https://doi.org/10.1023/a:1008332132218. https://doi.org/10.1023/A:1008332132218.

Suleiman, Naziru, Zaleha Othman, and A Ahmi. 2017. "Corruption: A Combat without Bullet, the Nigerian Economic and Financial Crimes Commission’s (EFCC) Perspective." *Asian Journal of Multidisciplinary Studies* 5 (7): 200-210.

Sutherland, Ewan. 2017. "Governance of Cybersecurity-the Case of South Africa." *African Journal of Information and Communication* 20: 83-112.

SWIFT. 2019. *Three Years on from Bangladesh: Tackling the Adversaries*. April 2019 ed. *Swift ISAC Report*. La Hulpe: Society for Worldwide Interbank Financial Telecommunication.

Symantec. 2016. *Cyber Crime & Cyber Security Trends in Africa*. Mountain View, CA: Symantec.

---. 2017. *Internet Security Threat Report*. Vol. 22. Symantec.

---. 2019. *Internet Security Threat Report*. Vol. 24. Symantec.

Tade, Oludayo. 2013. "A Spiritual Dimension to Cybercrime in Nigeria: The ‘Yahoo Plus’ Phenomenon." *Human Affairs* 23 (4): 689-705.

Tade, Oludayo, and Oluwatosin Adeniyi. 2016. "On the Limits of Trust: Characterising Automated Teller Machine Fraudsters in Southwest Nigeria." *Journal of Financial Crime* 23 (4): 1112-1125.

---. 2017. "‘They Withdrew All I Was Worth’ Automated Teller Machine Fraud and Victims’ Life Chances in Nigeria." *International Review of Victimology* 23 (3): 313-324.

The Council of Economic Advisers. 2018. *The Cost of Malicious Cyber Activity to the U.S. Economy*. Washington D.C.: Executive Office of the President.

The Economic Times. 2017. "Cyber Coordination Centre Made Operational: It Minister." *The Economic Times*, 2017.

---. 2018. "94% of Engineering Graduates Are Not Fit for Hiring, Says This It Stalwart." *The Economic Times*, 2018. https://economictimes.indiatimes.com/jobs/real-threat-of-ai-displacing-jobs-telecom-secretary/articleshow/68562762.cms.

The Executive Office of the President. 2018. *National Cyber Strategy of the United States of America*. Washington D.C.: The Whitehouse.

The Law Library of Congress. 2018. *Regulation of Cryptocurrency around the World*. Washington D.C.: The Law Library of Congress, Global Legal Research Center.

Trautman, Lawrence J. 2014. "Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?".

Trend Micro. 2016a. *Cybercrime and the Deep Web*. Trend Micro, Incorporated.

---. 2016b. "The Many Faces of Cybercrime." https://web.archive.org/save/https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-many-faces-of-cybercrime.

Ukpong, OU, and Akam Friday Uke. 2016. "Cashless Economic Policy and Sustainable Development in Nigeria Economy: The Missing Links." *Journal of Educational Policy and Entrepreneurial Research, 3 (3)* 3 (2012): 80-86.

Umarhathab, Syed, G Deepak Raj Rao, and K Jaishankar. 2009. "Cyber Crimes in India: A Study of Emerging Patterns of Perpetration and Victimization in Chennai City." *Pakistan Journal of Criminology* 1 (1): 51-66.

Urano, Akira. 2015. *North the Japanese Underground. Trendlabs Research Paper*. Los Angeles: Trend Micro.

Uthman, Ahmad Bukola, Lukman Adebayo Oke, Mohammed Kayode Ajape, Zayyad Abdul-Baki, and Murhtala Oladipupo Tijani. 2015. "Curbing Financial Crimes with Anti-Graft Bureaus in Nigeria: The Accountants' Perception." *Accounting and Management Information Systems* 14 (1): 107.

van Niekerk, Brett. 2017. "An Analysis of Cyber-Incidents in South Africa." *African Journal of Information and Communication* 20: 113-132.

van Wegberg, Rolf. 2020. "Outsourcing Cybercrime." PhD, Technische Universiteit Delft.

van Wegberg, Rolf, Jan-Jaap Oerlemans, and Oskar van Deventer. 2018. "Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin." *Journal of Financial Crime* 25 (2): 419-435.

van Wegberg, Rolf, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel Van Eeten. 2018. "Plug and Prey? Measuring the Commoditization of Cybercrime Via Online Anonymous Markets." 27th {USENIX} Security Symposium ({USENIX} Security 18).

Vasek, Marie, and Tyler Moore. 2015. "There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams." International conference on financial cryptography and data security.

---. 2018. "Analyzing the Bitcoin Ponzi Scheme Ecosystem." International Conference on Financial Cryptography and Data Security.

Vidal, Chaz, and Kim-Kwang Raymond Choo. 2018. "Situational Crime Prevention and the Mitigation of Cloud Computing Threats." Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13.

Wall, David S. 2013. "Policing Identity Crimes." *Policing and Society* 23 (4): 437-460.

Warren, Steve, Gavin Oxburgh, Pam Briggs, and David Wall. 2017. "How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?" International Conference on Human Aspects of Information Security, Privacy, and Trust.

Weber, Julia, and Edwin W Kruisbergen. 2019. "Criminal Markets: The Dark Web, Money Laundering and Counterstrategies-an Overview of the 10th Research Conference on Organized Crime." *Trends in Organized Crime*: 1-11.

White, Lawrence H. 2014. "The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-Gold." *Cato J.* 34: 281.

Whitty, Monica T, and Tom Buchanan. 2012. "The Online Romance Scam: A Serious Cybercrime." *CyberPsychology, Behavior, and Social Networking* 15 (3): 181-183.

Whitty, Monica T, and Magdalene Ng. 2017. "Literature Review for Underware: Understanding West African Culture to Prevent Cybercrimes. Report for the National Cyber Security Centre as Part of a Group of Studies Funded in the Research Institute in Science of Cyber Security."

Wilhoit, Kyle, and Stephen Hilt. 2015. *North American Underground: The Glass Tank*. *Trendlabs Research Paper*. Los Angeles: Trend Micro.

Wilk, Ryan. 2017. "The Ripple Effect of Identity Theft." *IQ: The RIM Quarterly* 33 (2): 36.

Williams, Matthew. 2006. *Virtually Criminal: Crime, Deviance and Regulation Online*. Routledge.

Wörner, Dominic, Thomas Von Bomhard, Yan-Peter Schreier, and Dominic Bilgeri. 2016. "The Bitcoin Ecosystem: Disruption Beyond Financial Services?".

Wu, Ke, Spencer Wheatley, and Didier Sornette. 2018. "Classification of Cryptocurrency Coins and Tokens by the Dynamics of Their Market Capitalizations." *Royal Society open science* 5 (9): 180381.

Xie, Rain. 2019. "Why China Had to Ban Cryptocurrency but the Us Did Not: A Comparative Analysis of Regulations on Crypto-Markets between the Us and China." *Wash. U. Global Stud. L. Rev.* 18: 457.

Zaytoun, Henry S. 2018. "Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft." *North Carolina Law Review* 97: 395.

Zhdanova, Maria, Jürgen Repp, Roland Rieke, Chrystel Gaber, and Baptiste Hemery. 2014. "No Smurfs: Revealing Fraud Chains in Mobile Money Transfers." 2014 Ninth International Conference on Availability, Reliability and Security.

Zimba, Aaron, Zhaoshun Wang, and Mwenge Mulenga. 2019. "Cryptojacking Injection: A Paradigm Shift to Cryptocurrency-Based Web-Centric Internet Attacks." *Journal of Organizational Computing Electronic Commerce* 29 (1): 40-59.

Section II: Lessons from the Russophone Literature

Introduction

The cybercrime literature, including Russophone cybercrime literature, focuses on evolving threats, gaps in legislation, and responses to criminal activities. However, only a few studies discuss the financial dimensions of cybercrime, such as the types of transactions and payment systems criminals prefer and what they do with the proceeds of their crimes. This section looks at the state of knowledge in the Russophone cybercrime literature. Consistent with the English review, the first part of this section discusses the methodology used to locate and review relevant articles. The second part contains an overview of the government bodies, information security companies, as well as academic and other organisations involved in researching and combating cybercrime. The third part presents the results of our review, focusing on the existing knowledge of cybercrime ecosystems in Russia, details of financial and business models used by criminals, and types of responses to disrupt these ecosystems. In conclusion, we discuss the limitations of these studies and ways to move forward given that the findings presented in this review can be valuable to researchers, industry experts, law enforcement, and further research or comparative analyses.

Key findings

Every year Russia loses hundreds of millions of rubles to cybercrime, including indirect costs of recovery from attacks and investigations (Verevkin and Verevkin 2017). Our review indicates that the existing literature on and knowledge of financial cybercrimes in Russia may have significant statistical gaps for two main reasons. First, small theft crimes tend to go unnoticed by the police; and, second, banks prefer not to report financial crimes.

The cybercrime market in Russia is very versatile. It includes numerous hacker groups, methods, and targets. If there is one common trait, it is that cybercriminals follow opportunities that yield money and, when they find safer ways to earn it, they start pursuing these opportunities both inside and outside Russia. Our review also shows that criminal behaviour is influenced by economic factors, including currency devaluation and exchange rates. However, few state-backed cybergroups stand out because they are rarely motivated financially and, instead, attack victims for disruption and sabotage purposes. Cybercrime methods have been evolving and will continue to attract criminals with low expertise, including members of traditional organised crime groups.

There is evidence to suggest that hacker groups experience high longevity. When members or even leaders of a group get arrested, the remaining members reorganise and continue operations. Low-scale fraudsters are most likely to operate only in Russia, while large groups do not have a particular focus on the region and attack victims in other countries. Once tools and schemes are successfully applied in Russia, they are exported to target victims abroad, usually starting with the Commonwealth of Independent States (CIS) countries. Transactions that coerce victims to pay money or are the result of digital theft of money are most common.

Social engineering and phishing remain the modus operandi for cybercriminals in Russia because these methods are comparatively easy to execute and do not require much expertise. Social engineers bet on human error, computer illiteracy, and gullibility; these types of attacks are numerous, but the average amount stolen is usually small. These offences, as well as data theft, seem to be a low priority for Russian banks that prefer focusing on processing security, SWIFT transfers, and ATMs security, because those breaches result in larger thefts. While criminals heavily rely on social engineering, banks and regulators often put the onus on the victims, highlighting victims' poor computer and cyber literacy.

Russian law enforcement lacks the capacity and training necessary to investigate cybercrime and the use of virtual currencies. Accordingly, the majority of cybercrimes in Russia goes unnoticed by regulators and the police; consequently, many experts characterise cybercrime as highly hidden in the Russian context. Estimating losses from cybercrime presents further challenges, which may be the reason why the Central Bank of Russia and industry experts, such as Positive Technologies and Group-IB, sometimes publish discrepant data.

Most Russian cybercriminals operate with fiat currencies, principally the Russian ruble. Fiat currency can be easily moved and laundered with the help of facilitators in financial organisations or money mules. Offenders usually execute multi-step transferring operations in and outside Russia, using traditional bank transfers, as well as e-payment systems with anonymous wallets to cash out. Such operations can involve dozens of people. Virtual currencies are principally used in specific crimes such as extortion, ransom, or purchasing goods and services on the dark web. It is not likely that criminals exchange their fiat proceeds into cryptocurrencies *en masse*, even though a lack of legislation and knowledge regarding cryptocurrencies prevent Russian law enforcement from confiscating crypto wallets.

Methods

This report provides a systematic review of extant Russophone research and English-language research on Russian cybercrime, both in terms of the academic and grey literature, on criminal transactional methods in cyberspace. The objective of this review is to outline the state of knowledge within the area of criminal transactional methods, as summarised by Russophone researchers, academics, governmental agencies, and leading information security companies. Acknowledging the lack of previous in-depth research on illicit transactional methods in Russia, we surveyed various sources, including policy analyses, industry reports, conference proceedings, and news articles. Our review will also include government and think-tank reports and investigations. Consistent with the English review, we only retrieved articles, reports, books, book chapters, and other relevant publications that are in the public domain, free to access, or accessible with a university subscription from 2013 onwards.

We began our research by creating a list of search terms to use throughout our work. The English review keywords were a good starting point; however, we had to change some of them, according to Russian linguistic online culture and common use of the terms on the subject. For instance, the central umbrella term ‘cybercrime’ has two Russian translations: *киберпреступление* and *киберпреступность*. The former refers to specific types of crimes conducted with the means of the internet, while the latter means criminality and criminal activities in general. To capture a wide range of literature, we used both Russian terms in our searches.

In the early stages of our research, we also noticed that legal, police, and academic experts used other terms to refer to cybercrime. The two terms most frequently used were *киберзащита* (cybersecurity) and *информационная безопасность* (information security). Moreover, there is an ongoing criminological discussion on which terms to use in research and publications. Some criminologists suggest avoiding the term *киберпреступление* (cybercrime) altogether, as it is too narrow and inapplicable to certain crimes in a Russian context. Instead, they propose using terms such as *компьютерная преступность* (computer crime) or *преступления в сфере компьютерных технологий* (computer technology crime) (Shevchenko 2014; Khaliullin 2014; Komarov 2016). With these suggestions in mind, we then modified our searches accordingly. In Appendix 1, we present our finalised keyword list.

Using the keyword list, we first searched eLibrary[21], Russia’s biggest digital library, containing academic journals, publications, and conference papers. In addition, we reviewed all bibliographies for the articles retained from the search strategy. Second, we looked at specialised criminology journals, specifically The Lawyer publishing group («Юрист»): *Law and Cybersecurity* («Право и кибербезопасность»), *Expert Criminologist* («Эксперт-криминалист»), *InformationLaw* («Информационное право»), and *Financial Law* («Финансовое право»). Third, we looked at credible Russian universities (such as the Moscow State University[22] and the Higher School of Economics[23]) and think-tanks (Carnegie Moscow Centre[24], Institute of World Economy and International Relations (IMEMO)[25], Association of Independent Centres for Economic Analysis[26]). This search strategy generated the least amount of available reports and publications.

Fourth, we targeted government entities and state companies (Ministry of Internal Affairs[27], FSB[28], Roskomnadzor[29], Minkomsvyaz[30], Rostelekom[31], Central Bank of Russia, and Sberbank[32]) to identify departments whose main line of work involves dealing with cybercrime and cybersecurity. The four most relevant departments were Department K of the Ministry of Interior’s Bureau of Special Technical Activities (Управление «К» БСТМ МВД), Central Bank’s FinCERT department (ФинЦЕРТ), Rostelecom’s security operations centre, and Sberbank’s subsidiary BI.ZONE (cybersecurity and threat intelligence company).

To expand on the legal aspects of legislating and regulating cybercrime in Russia, we looked at the largest legal database in Russia, *Consultant («*Консультант»*)*[33]. *Consultant* provides legal reference information, including different levels of legislation, court rulings, and scientific articles. The keyword search on the website identified 48 relevant academic publications.

Finally, we needed to identify leading information security companies in Russia. To do that, we looked at one of the most respectable business news media outlets in Russia *Kommersant* that codes its publications by themes[34]. Having checked a number of articles under the information security theme, we found major Russian companies that investigate cyberthreats and cybercrime. These include Group-IB[35], Solar JSOC[36], Positive Technologies[37], Jet Infosystems[38], Kaspersky Lab[39], and Qrator labs[40]. Conducting keyword searches on these companies’ websites helped us to draw publicly available reports and publications; however, none of them contained any methodology across data collection applied by the industry analysts to conduct research.

The search yielded 144 publications, journal articles, books, reports, and news items. In the following review, we retained 111 of these publications. The studies that were excluded did not provide novel insights, were not supported, or contained a generic overview of cybercrimes.

Our initial search strategy was aimed to retrieve literature in Russian. Results were Russia-centric, unsurprising as Russia is the largest country where Russian is spoken. While there are other Russian speaking regions, such as Belarus, parts of Kazakhstan, Latvia, Ukraine, Tajikistan, and other former Soviet states, we did not include them in our study for two major reasons. First, users in these countries represent a small proportion of Russophone internet users. Second, to specifically include countries other than Russia, we would have to modify our keyword search to include those countries to find relevant literature; it became evident that Russophone cybercrime research does not focus on these countries in any significant way. However, some Russia-based hackers target Russian speaking regions outside Russia, which we discuss in our review below. However, according to our findings, large hacker groups are usually multinational and target many countries besides Russia.

The following section provides an overview of law enforcement, financial regulations, and political considerations that help to contextualise Russian cybercrime infrastructure and strategies. We then turn to an overview of the empirical results from the Russophone literature review.

The State of Play in Russia

This section provides an overview of the relevant cybercrime regulations and bodies in Russia.

Cybercrime

With 110 million internet users, Russia’s most common types of cybercrime are similar to those experienced elsewhere where internet usage and penetration are high: online money theft, terrorist propaganda, and cyber espionage. The losses from cybercrime in 2015 in Russia were estimated to be from 4 to 5 billion USD, and the rate of crimes is growing (Timofeev 2016). According to the Prosecutor General Yuri Chaika, between 2013 and 2016 the number of cybercrimes increased six-fold (RIA Novosti 2017a). In 2018, the number of critical incidents, including those that allow criminals to obtain more than one million Russian rubles (15,300 USD[41]) per one session, increased by 19% (Solar JSOC 2019).

Despite the fact that one in four Russians claims to have experienced a cybercrime attack in the last 24 months (PwC 2018), Russian authorities often approach cybercrime as if it is only an external threat to the state’s stability rather than a threat to its ordinary citizens as well. In the Information Security Doctrine, ratified by President Vladimir Putin in 2016, the main threat in cyberspace is said to come from ‘individual states’ with technological superiority and intelligence services that want to destabilise Russia politically (Pravo.gov.ru. 2016). Less of a threat, according to the Doctrine, are terrorists engaging in cybercrime, and, finally, ordinary hackers who steal personal data of Russian citizens and money from their bank accounts. The same Information Security Doctrine states that Russia’s technological development lags behind that of many other countries and is heavily dependent on foreign software. Consequently, Russian authorities state that Russia cannot yet participate in the management of global cyberspace. Nevertheless, the Russian National Security Strategy notes that achieving information superiority in cyberspace by 2020 is an essential goal (Kremlin.ru 2009).

Russia has not acceded to the Council of Europe’s Convention on Cybercrime, known as the Budapest Convention (RIA Novosti 2017b). The Russian government has criticised the document for many years claiming that certain articles of the Convention threaten state sovereignty and thus should be changed or removed completely (TASS 2017).

Russia has proposed replacements to the Budapest Convention. In 2011, Russia prepared a draft UN Convention on International Information Security which covered warfare in cyberspace, cyberterrorism, and cyber fraud. The United States and the European Union strongly opposed the document. Then, in 2017, Russia’s Ministry of Foreign Affairs presented another draft UN Convention on Cooperation in Combating Information Crimes (Chernenko 2017). Finally, in December 2018, the UN General Assembly adopted a Russian resolution on international information security titled ‘Developments in the field of information and telecommunications in the context of international security’. The document reflects Russian government views on information security: it underlines the commitment to use information and communications technology exclusively for peaceful purposes and to respect the sovereignty of states in the information space. The United States and the EU countries voted against the resolution (Ministry of Foreign Affairs of Russia 2018).

Numerous reports suggest that Russian authorities interfere with other states’ affairs using cyber methods – actions denied by Russian authorities (Goryashko 2019). Moreover, academic researchers Smirnova and Holt (2017) suggest that Russian hackers may try to engage in targeting foreign individuals and companies without the threat of being prosecuted domestically. However, Russian authorities also seek to regulate cyberspace within Russia and its citizens' use of it. One of the major steps in this direction was a bill that sought to isolate the Russian segment of the internet from international servers. Despite rallies and protests in several Russian cities (BBC 2019), the bill was approved by the Federation Council and signed by President Vladimir Putin on May 1, 2019 (Pravo.gov.ru. 2019).

Russia is also the country in which much of the malware used to attack people around the world is developed and from where cyber-attacks often emanate. Russia is a developed country with extensive technological education, meaning the skills required to develop such products are relatively highly possessed. According to European Union law enforcement investigations, half of the EU member states identified infrastructure for cybercrime, such as command and control servers and phishing domains, or suspects through the course of their investigations in four main countries: the Netherlands, Germany, Russia, or the UK (Europol 2015). Additionally, one third of the EU states found cybercrime similar infrastructure or suspect links to 12 other European countries, including Ukraine and Latvia which are countries where Russian is widely spoken. According to the same report, a lack of judicial cooperation between the EU member states and Russia presented one of the major difficulties in investigating cybercrime.

Russian cybercriminal groups appear to be active in the United States as well. Specifically, the US Department of Homeland Security and the FBI attributed two cyber espionage groups APT28 (aka Fancy Bear) and APT29 (aka Cozy Bear) to Russian intelligence services (Homeland Security 2017). Among other things, these groups are said to have started a spear-phishing campaign targeting US candidates, as well as the Democratic National Committee (DNC) in the 2018 midterms and shortly after. Both cyber espionage groups have reportedly targeted governments, the military, international organisations, and think tanks in the United States and Europe (Symantec 2018a).

Overall, cyber-groups backed by the Russian government do not seem to focus on extracting currency directly. Espionage, service disruption, trolling, and data theft are the most frequent cybercrimes committed by such Russian actors. The high rate of these crimes is mostly due to their low costs and low risks, as well as a use of proxies in overseas operations that can be denied later by Russian officials (Borogan and Soldatov 2018).

Russian darknet marketplaces present another global threat. There, offenders can store, buy, and sell various tools and materials required to commit various types of cybercrime, including computer hacking tools and kits, personal data records, and malware (INTERPOL 2018; Zakharov 2019). Europol also reported that most online marketplaces with child sexual exploitation materials (CSEM) were Eastern European or Russian marketplaces. To gain access to these markets, users either need to provide CSEM or pay money (Europol 2018).

There are also darknet drug marketplaces, such as RAMP (Russian Anonymous Marketplace). Before it was shut down in 2017, RAMP had been one of the largest drug markets in the world, ran almost exclusively in Russian, and used a classic forum structure (Europol 2018). According to its creator, in 2014, with 14,000 active buyers and sellers, RAMP made around 250,000 USD. It did not take a commission on drug sales but charged dealers 300 USD monthly for a prime spot on its home page and an extra 1,000 USD a month for a 'license' to sell cocaine, hash, and amphetamines in the Moscow market (Greenberg 2014). The Russian authorities claimed that they had shut down RAMP but did not report how they managed to do it or whether they made any arrests. This lack of details led some experts to suggest that the law enforcement did not actually shut down the service; instead, the owners or the new management might have left the project with all the money (Levchenko 2017). Moreover, the police later clarified that, in fact, they had only terminated operations of a few drug-dealing organised groups that had stores on RAMP (Sologub 2017). Till the present day, it is still unclear why the whole platform ceased its business. One of the former store owners on RAMP anonymously told journalists that he moved his drug business to another platform but did not specify which one (Abrosimova 2017). Most buyers and sellers likely went to the Russian speaking marketplace called Hydra (Sologub 2017; Kumachev and Nogayeva 2018). Finally, Telegram messenger became another platform with a drug trafficking infrastructure, including closed discussion groups, individual sellers, and chat bots (Persianinov 2017).

When it comes to international cooperation, cybercrime appears to be yet another area where Russia and the West disagree with each other, thereby limiting their willingness to form partnerships. Nonetheless, Russia cooperates with the Commonwealth of Independent States' members[42] on combating cybercrime. For example, according to the 2016-2020 Programme, the countries aim to further develop international legal norms, participate in joint operations and training exercises, and cooperate in the training of specialists (Commonwealth of Independent States 2016). Similar agreements have been made with the countries of the Shanghai Cooperation

Organisation[43] (2018). However, it is challenging to evaluate the effectiveness of such cooperation.

Additionally, Russia appears to be more open to partnerships with Western counterparts when they target specific crimes. For example, the Russian Ministry of Interior joined Europol's project 'No more ransom' aiming to help victims of ransomware (Europol 2016). The website has a Russian version, which, according to the ministry, makes the information on the website relevant for Russian citizens (Ministry of Interior 2017).

Europol (2018) indicates that Russia is among a few countries in Europe that largely experience malicious emails as an attack vector to get a victim to download malware. Malicious emails are reported to be the most commonly detected cyber-attack technique (PwC 2018). The rising use of malware in cyber-attacks in the last two years (mostly for espionage and remote control) is linked to such malware becoming cheaper to obtain and thus attracting more criminals (Positive Technologies 2018c). Additionally, Symantec ranked Russia the fourth largest initiator of internet of things (IoT) attacks in the world between 2016 and 2018, after China, the United States, and Brazil (Symantec 2018b; 2019).

Socially engineered frauds and scams have been common in Russia for many years (Bank of Russia 2017; Bank of Russia 2018; Positive Technologies 2018c). The Central Bank of Russia reported that, in 97% of fraudulent cases involving bank cards, victims are manipulated into transferring their own funds to another account or into revealing their personal banking information via a phone call. Offenders use IP telephony (Session Initiation Protocol, or SIP) that spoofs an incoming call to look like a real bank's phone number so that victims are more likely to trust the callers. In 2018, it is estimated that 1.4 billion roubles (21.7 million USD) were stolen from Russian bank cards alone (Bank of Russia 2018). Every day around 950 people become phishing victims in Russia and the Commonwealth of Independent States (Group-IB 2017).

Russian cybercriminals may be a part of a bigger organised crime group that commits traditional crimes, such as fraud, theft, extortion, and the production of child exploitation materials (Veprev and Nesterovich 2018). However, there has been no significant research on the cybercrime and organised crime nexus.

The poor security of Russian online banking portals and banking apps presents another opportunity for cybercriminals. According to the Positive Technologies report, 61% of all Russian online banks have low or very low security systems in place, while

56% have vulnerabilities that can lead to fraudulent operations with individual funds, as well as money theft (Positive Technologies 2019).

Cybercrimes in Russia are often not prosecuted as cybercrimes per se due to the specifics of Russian laws and outdated terminology. The Ministry of Interior also states that cybercrimes are often prosecuted as fraud which makes cybercrime more latent for the law enforcement (RIA Novosti 2018b). Russian legislation on cybercrime has not been updated since its adoption in 1996 when cybercrime was referred to as 'computer information' crime[44] (Veprev and Nesterovich 2018). Article 159.6 titled 'Fraud in the field of computer information' is another article in the Criminal Code which is often used to prosecute crimes, such as money theft from bank accounts and e-wallets, including crimes conducted with previously obtained personal data (Nikulina 2015; Sharova 2017; Lebedeva 2018a; 2018b).

Russian governmental bodies charged with investigating or policing cybercrime rarely produce publicly available reports of any kind. Some statistics can be found in omnibus annual reviews, interviews with heads of such bodies, or in media coverage of events and conferences on cybersecurity. Most opensource information available is published by private security and research companies.

The law enforcement, public service, intelligence, and investigative bodies that work on cybersecurity and cybercrime in Russia include:

- **Security Council of the Russian Federation** (Совет безопасности Российской Федерации). The Security Council presents the findings of monitoring the implementation of the Doctrine of Information Security to the President.
- **Ministry of Interior's Bureau of Special Technical Activities, Department K** (Управление «К» БСТМ МВД). This department deals with online fraud, computer information security, malware, and other instances of cybercrime in Russia. For the general public, the department issues general guidelines on cyber-safety that cover issues like the safe use of bank cards, social engineering, and ATM safety.
- **The Federal Service for Supervision of Communications, Information Technology, and Mass Media, Roskomnadzor** (Роскомнадзор). Roskomnadzor is a federal executive authority performing the following functions: control and supervision of mass media (including electronic mass media), mass communications, information technology, and telecommunications; supervision and statutory compliance control of personal data processing; and management of the Radio Frequency Service activities. More commonly, it is the main censorship body in Russia as it has the power to block websites through internet providers.

- **Ministry of Telecom and Mass Communications of the Russian Federation, Minkomsvyaz’** (Минкомсвязь). Minkomsvyaz’ is responsible for developing and implementing national policy and legal regulation in telecommunications, information technology, personal data processing, and internet governance.
- **GOV-CERT.** GOV-CERT is a cyber security and incident response team for Russia’s governmental networks. GOV-CERT aims to coordinate state authorities, local authorities, and law enforcement units for the identification, prevention, and removal of the consequences of computer incidents.
- **RU-CERT.** RU-CERT is a computer security incident response team that provides computer incident prevention and response service for all users in Russia.
- **The Financial Sector Computer Emergency Response Team, FinCERT** (ФинЦЕРТ). FinCERT is part of the Central Bank of the Russian Federation. It exchanges information among the Central Bank, banks, non-bank financial institutions (NBFIs), integrator companies, anti-virus software vendors, and communications service providers and operators, and specifically law enforcement and other public authorities overseeing cyber security across the industry. It analyses data about cyber-attacks on banks and NBFIs and issues information protection guidelines for the safe transfer of funds.
- **Rostelecom** (Ростелеком). Rostelecom is Russia’s largest digital service provider with 50% of its shares owned by the state. Rostelecom has its own SOC (security operations centre) with 50 employees who monitor cyber-threats 24/7. The 2017 yearly report notes that Rostelecom cooperates with Russian executive governmental bodies on information technology issues (Rostelecom 2017, pp.98-99).

Financial Crime

Russia has been a member of FATF since 2003. It is also a member of:

- EAG – the Eurasian Group on Combating Money Laundering and Financing of Terrorism;
- MONEYVAL – a Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism;
- Egmont Group – a united body of 164 Financial Intelligence Units around the world.

Asset misappropriation remains the most common type of economic crime in Russia, followed by bribery, corruption and fraud in the procurement sphere. Of the Russian respondents, 66 % reported being victims of economic crime, which is significantly higher than the global average of 49% (PwC 2018).

Russia ranks 138 out of 180 in the Corruption Perceptions Index calculated by Transparency International. Russia has a long history of money laundering. The IMF (2016) indicates that the current understanding of money laundering and terrorism financing in Russia may be limited because it mostly relies only on analysis from the banking sector and overlooks criminal proceeds in other sectors, such as real estate, law firms, and precious metals and stones.

In Russia, cryptocurrencies and operations with them are a regulatory grey zone. While cryptocurrencies are not illegal, operations involving cryptocurrencies may be checked for money laundering or financing terrorism (Rosfinmonitoring 2014). As of August 2019, the State Duma (the lower house of the Federal Assembly of Russia) is still reviewing a bill on cryptocurrencies and their regulation. In the proposed document, mining would not be regulated until a mining individual exceeds state electricity usage rates per person for more than three months (Duma.gov.ru 2018). At that point, mining would be classified as an entrepreneurship for which a person should have a license and pay taxes.

The main organisations tasked with combating financial crime in Russia are:

- **The Federal Financial Monitoring Service of the Russian Federation, Rosfinmonitoring** (Росфинмониторинг). Rosfinmonitoring is considered Russia's main body for financial intelligence. It was founded in 2001 as part of the Ministry of Finance and, since 2004, has been an independent body which reports to the government.
- **Federal Security Service, FSB** (ФСБ). The FSB has some departments that deal with financial crime, including Department ‘K’ (Information Security Centre) which is part of the Counterintelligence Unit. Usually most FSB activities and its staff are classified.
- **Ministry of Interior’s Department for Economic Security and Combating Corruption** (Главное управление экономической безопасности и противодействия коррупции МВД). This department investigates laundering of illegally gained funds, regional and international tax evasion, financing of terrorism and extremism, and other crimes.

Review of the Russophone Cybercrime Literature

The Russian-language review resulted in the retention of 111 manuscripts, peer-reviewed articles, government and industry reports, book chapters, news publications, and conference proceedings. The retrieved body of academic literature primarily consisted of broad overviews of cybercrime, including conceptual, linguistic, and legal aspects, as well as law enforcement responses to cybercrime. The majority of works still regarded cybercrime as an emerging type of crime in Russia and did not present in-depth analyses of specific threats and types of offenders. However, information security companies, such as Positive Technologies, BI.ZONE, and Group-IB, as well as the Central Bank's FinCERT, contained a sufficient amount of quantitative and qualitative data, original research, and intelligence. As a result, many academic authors whose works we reviewed often included these companies' analyses in their studies as the only source of statistical data. Additionally, the majority of these works, especially those covering cryptocurrencies, discussed foreign practices and cases which examine different dimensions of cybercrime, perhaps also due to the lack of research on the subject in Russia.

In coding the literature on cybercrime business models, types of transactions, and their regulations in Russia, we found themes that were consistent with the codes in the English language review. However, as we started reviewing the Russophone literature, we added new codes that were not included in the English review. First, because there was more information available on victims than perpetrators of cybercrime, we created a code for victims of cybercrime, both individuals and companies, to see how attacks differ for each. Second, we used the behavioural characteristics theme as a foundation for discussing a cybercriminal profile and evolving criminal methods. Third, we created sub-codes for cryptocurrency mining and DDoS attacks because many authors discussed them frequently.

Accordingly, we present the findings thematically as follows. First, we explore criminal ecosystems and contextualise them with a cybercriminal profile and behavioural characteristics. Second, we look at criminal marketplaces on the dark web, followed by the aspects of crimeware-as-a-service. Finally, we consider specific types of crimes for financial gain, such as fraud and theft, data theft, ransom, extortion, and cryptojacking.

In the next subsection, we discuss the proceeds of cybercriminals and the specifics of transactions with different currencies (fiat, virtual, and digital). This is followed by the typology of transactions in which criminals can be involved and transactional facilitators. We close this section with an overview of and a discussion on relevant legal and financial regulations in Russia.

The findings that we present in the following sections are Russia specific unless specified otherwise. We also share comparisons with other countries and markets where possible.

Criminal Ecosystems

Cybercriminal profile

Russia has a long history of cybercrime. Poor economic prospects coupled with people who possess high technical skills encourages black-hat activity (Bayoumy 2018; Kraemer-Mbula, Tang, and Rush 2013). One historical Russian-linked cybercriminal operation was the Russian Business Network (RBN) that was linked to a myriad of cybercrimes (Kraemer-Mbula, Tang, and Rush 2013).

Cybercriminals in Russia are rarely loners, nor are they members of a homogeneous group that specialise in one aspect of a crime (Khaliullina 2018). Typically, cybercriminal groups consist of 5 to 7 members with different roles and responsibilities, such as attack coordinator, programmers who deal with malware, and money mules (Timofeev 2016; Verevkin and Verevkin 2017). However, groups can be larger depending on the type of attacks. According to publicised cases, groups that use malware for theft may have up to 20 members (Lebedeva 2018a). Successful criminal gangs who target banks ‘resemble IT companies backed by a well-coordinated team of hackers’ (BI.ZONE 2019, p. 43). It is also likely that criminal groups outsource some tasks to freelancers who may not know about the final goal or the identity of the people subcontracting them (Group-IB 2018b).

The leaders of these groups (coordinators) may not have any programming skills, and their only responsibility is to put together an efficient team. A group’s structure and division of roles can later complicate legal investigations because it is hard to establish individual responsibilities (Positive Technologies 2018a). When big hacker groups are disrupted by arrests or for other reasons, the remaining members continue attacks or reorganise into new teams[45] (Group-IB 2018a; BI.ZONE 2019).

Russian cybercriminals may be a part of a larger organised crime group that commits traditional crimes, such as fraud, theft, extortion, and the production of child exploitation materials (Veprev and Nesterovich 2018; Positive Technologies 2018c). It is getting easier to become a cybercriminal without any expertise, since one can buy the necessary tools and instructions on the dark web (Positive Technologies 2018a). The first example in Russia was the 2005 creation of Zeus, the first point-and-click program to create and run a command and control structure on a botnet (Bottazzi and Me 2015). Moreover, carrying out certain attacks is becoming simpler due to their partial or full automation, as in the case of phishing attacks. Automation appears to have resulted in a modest expansion in the number of groups using phishing as an attack vector from 2017 to 2018 (Group-IB 2017; 2018a).

When attacks require more expertise and investment in technology, as well as when they come with higher risks, there appear to be fewer, more specialised groups engaging in that behaviour. In 2017, there were only two groups who performed targeted attacks on banks (three in 2018) and three groups who targeted online banking systems using malware (Group-IB 2017; 2018a).

Nationality and the exact location of the cybergroup members are hard to identify without making any arrests; however, the Group-IB research shows that all financially motivated cybergroups who target banks in Russia are Russian-speaking groups (Group-IB 2018a). On stolen data markets, it is plausible that a substantive proportion of participants are also Russian nationals who most likely reside near or in Russia while targeting other countries to avoid domestic prosecution (Smirnova and Holt 2017). Age-wise, the research shows that criminals can be anywhere from teens to over 60 (BI.ZONE 2019). However, some types of criminals have become older. In 2018, 41% of dummy bank cards were issued to Russians under the age of 25, while in 2019, this number plummeted to 21%.

While some researchers suggest that Russian hackers avoid attacking Russian individuals and companies to avoid being arrested by Russian authorities and prefer targeting foreign nationals and companies in the United States and some EU countries (Digital Shadows Photon Research Team 2019; Smirnova and Holt 2017), there is substantial evidence suggesting that Russian hackers operate on any market with sufficient demand and that they ‘follow the money’ (Group-IB 2018a, p.22). Since very few cybercriminals targeting Russian banks and citizens ever get caught and prosecuted, and since few people report cybertheft to the police[46] (Lavronenko 2018b), it seems unlikely that cybercriminals are deterred by domestic legal repercussions. Moreover, industry experts have found evidence that fraudulent schemes and attacks once tested in Russia are later ‘exported’ for application in other countries (Group-IB 2017; Kaspersky 2019). For example, as of 2017, all criminal groups that attacked Russian banks in the past gradually turned their attention to other countries in Europe, Latin America, Asia, the United States, and the Middle East (Group-IB 2017). Some of these groups continued successful attacks on financial institutions in Russia.

While big Russian-speaking cybergroups may have no obvious focus on any region[47], there are geographical patterns of cybercrime distribution inside Russia. As reported by the Central Bank of Russia (2019), the Central Federal District[48] has the highest rate of payment card crimes due to the largest number of financial organisations located there. Two thirds of all unsanctioned operations with bank cards aimed at money theft take place in Moscow.

Economic factors also affect criminal behaviour. During the extreme devaluation of the Russian ruble in late 2014 and early 2015, three out of five cybercrime groups who specialised in money theft from companies reportedly left the Russian market in favour of countries in Western Europe (Timofeev 2016). During that period, experts observed an almost threefold decrease in money theft in the Russian internet banking sector. Group-IB (2017) predicted that hackers would further monitor cash flows collecting compromising information about bank clients, as well as disrupting internal infrastructure processes.

Big international events can lead to a spike in cybercriminal activity. During FIFA-2018 held in Russia, the Central Bank of Russia recorded 9 attacks on ATMs[49], 19 mass emails with malware, 3 DDoS-attacks, and 2 mass emails with extortion threats (FinCERT Bank of Russia 2018).

Russian criminals will explore new markets to find vulnerabilities they can exploit. Potential new victims of large-scale attacks include extracting industries with growing automation in their companies, and trading applications and services with weak security systems that allow quick monetisation (Zaernyuk and Chernikova 2017; Positive Technologies 2018a).

Evolving methods

Hackers in Russia are now choosing their victims more carefully than before. According to the Group-IB data, the number of groups in Russia aimed at committing theft and subsequently the number of attacks on companies had decreased by almost 50% in 2017 from the previous year, but the average loss per victim had increased (Group-IB 2017). In other words, there are fewer attacks but more profit per operation. This corresponds with the findings from PwC (2018) where percentage of responses reporting a cybercrime incident in Russia has not changed much during the last few years (from 23% in 2016 to 24% in 2018).

Cybercriminals prepare as thoroughly as possible before they attack. Some pretend to be legal start-ups or fintech companies. Under this disguise, they employ individuals and companies to conduct cybersecurity research on their potential victims to find their strengths and weaknesses. Moreover, cybergroups can spend up to 40% of their profits on further research which can help them in their future criminal activities (Verevkin and Verevkin 2017). Additionally, there has been an increase in attacks aiming to establish long-term control over a company's infrastructure so that criminals can research the company in detail for maximum profits (Solar JSOC 2018).

To achieve their goals, cybercriminals constantly change and improve their methods. For example, some use remote control tools instead of man-in-the-browser attacks; others prioritise obtaining bankcard data over SMS banking information[50]; while others decrease the use of Android-based trojans (Group-IB 2017; 2018a).

Another way to make attacks more complex and for criminals to bypass a company's security mechanisms is to attack via a third party (BI.ZONE 2019). The attacks on Unistream Bank in the autumn of 2018 are examples of multi-layered operations in Russia. First, criminals scammed the organisation with an email seemingly from an undisclosed large bank. Then, a month later, hackers infiltrated the bank's infrastructure to send out malicious emails on behalf of Unistream. The total losses incurred remain confidential. The primary suspect of these attacks was the Cobalt group (BI.ZONE 2019).

As technology evolves, criminals may use machine learning to gain their victim's trust. For example, extortionists can use machine learning to analyse their victim's style, preferences, and interests from social media (Kardakov and Gizatullin 2018). Afterwards, attackers serve victims with 'targeted' phishing links or websites that have content similar to the victim's social media pages.

While crimes conducted with the internet of things (IoT) devices in Russia are very rare for now, more criminals are likely to use them in the near future due to the vulnerabilities present in most IoT devices (Positive Technologies 2018a; BI.ZONE 2019). For instance, many companies and banks have printers, surveillance cameras, and other smart devices which can be attacked on their own or as a first step before a bigger attack (Kondrashin 2018).

Criminal Marketplaces

Underground criminal marketplaces provide a rich platform where one can find illegal tools and services, *inter alia*, for use in cybercrime. With cryptocurrency or fiat currencies via e-payment systems, criminals can purchase malware, ransomware, mining tools, exploits, personal data, and access to websites (Stoyanov 2015). It is unknown how many criminal markets, forums, and other types of platforms exist. Researchers and industry experts usually identify one or two dozen to analyse new threats and criminal activities. For example, Positive Technologies (2018b) found 25 popular Russian and English language platforms on the dark web with more than 3 million registered users altogether. Holt, Smirnova and Chua (2016) inspected 13 forums for stolen data that are operating around the world and whose users communicate in the Russian and English languages.

These analyses show that Russian cybercriminal marketplaces have diverse audiences. Some markets are clearly targeted to Russophone users, with posts written in Russian and Ukrainian and sporadically supplemented with English translations (Ablon, Libicki, and Golay 2014). Other research indicates that Russia hosts multilingual criminal forums, such as the long-standing forum, *The Hidden Answers* (Bayoumy 2018).

Within the forums, different tools and services have varying costs, supply, and demand. The two most popular services on the dark web among buyers are reportedly malware (55%) and services for hacking emails and websites (17%) (Positive Technologies 2018b). Such markets appeal to criminals because it is cheaper to buy or rent tech products for cyber-attacks from a third party than to develop a new tech product. Examples include:

- Financial malware. Financial malware is designed to steal account credentials. Through 2015 all deployments of financial malware that were traced to their origin were produced by Russian-based criminals (Cyphort 2015).
- Remote access trojans (RAT). RATs are used to access devices and control them remotely. The average price for this type of malware in 2017 was 490 USD. Gaining control over the website by hackers can cost from 150 to 1,000 USD. In 2017, buying access to online banking apps cost around 22 USD per client (Positive Technologies 2018b).
- DDoS attacks. A targeted DDoS attack can cost up to 4,500 USD and includes a hacker, rented infrastructure, and necessary tools. DDoS attack services on several of the Russian darknet markets cost 5 USD per hour, 50 USD per day, 200 to 350

USD per week, and 1,000 USD per month. Hackers charge more if the target website has anti-DDoS protection installed (SecureWorks 2016).

- Fraudulent website creation. Creating a simple copy of a website for phishing purposes costs from 50 to 150 USD, while making an authentic website with redirection to the original website to avert suspicions will cost up to 200 USD.
- Email compromise. Popular Russian email accounts such as Mail.ru, Yandex.ru, and Rambler.ru can be hacked for 65-103 USD (or as low as 40 USD). The price for Russian company dossiers ranges between 40,000 and 60,000 rubles (604-906 USD) (SecureWorks 2016, Positive Technologies 2018b). Social media accounts data are usually sold in bulks of thousands and even millions of entries for only dozens or a few hundred USD for the whole database (FinCERT Bank of Russia 2018).
- Bulletproof hosting. Bulletproof hosting refused to complaints about malicious content nor does it cooperate with police. It is used as a base for command and control operations and to host illicit content, such as child abuse materials.

Research on markets for stolen personal information shows that nearly any type of data can be stolen and sold quite cheaply (Smirnova and Holt 2017). Criminals can later use the stolen data to register on e-payment services and remain anonymous in their transactions (SecureWorks 2016; Positive Technologies 2018a; Positive Technologies 2018b). There are three main e-payment systems in Russia with millions of users combined: QIWI, WebMoney, and Yandex.Money. As of August 2019, there are anonymous and verified fiat e-wallets on these services with different rules regarding an account balance and operations with the account. Both types are usually linked to a mobile phone number, while the verified e-wallets are also linked to bank cards. One can top up e-wallets with cash at the automated kiosks, via online banking and bank transfers, and by transferring money from a phone number balance. With the stolen data, criminals can get verified e-wallets under someone else’s name and become untraceable. We elaborate on the general and criminal use of e-payment systems in the *Non-traditional transactors* section.

Carding on the dark web offers bank account and other personal information of bank clients to perform fraud services. Group-IB (2018a) reports that every month 686,000 text data of bank cards are uploaded to the online markets worldwide, along with 1.1 million card dumps (stolen electronic copies of cards that can be used as clones of real cards for unauthorised transactions). Text data per card on average costs 9 USD, while a dump costs around 33 USD (Positive Technologies 2018b). However, Russian news reports suggest that personal banking information can be many times cheaper when large amounts of data are stolen at once. The business newspaper *Kommersant* reported that breached personal data of 70,000 clients of Binbank were on sale on online black markets for 5 rubles per person (0.077 USD) (Goryacheva and Trifonov 2019).

Researchers and security experts have noticed that hackers operating on the Russian darknet forums advertise their outstanding abilities similarly to licit business (SecureWorks 2016). Many offer hacking services, highlighting the possibility to expand their working hours to include weekends and 24/7 availability, if necessary.

Like any other platform, many listings with advertised services on the dark web are fraudulent so that buyers have to be careful (Positive Technologies 2018b). Perhaps this is one of the reasons that the majority of sellers are now offering customers the ability to work through ‘guarantors’ who ensure that the exchange of data and payment take place fairly. Usually, for a small percentage, guarantors hold the money and the product before distributing it to both parties involved in the transaction (SecureWorks 2016). Cryptocurrency is used often for the exchange (Positive Technologies 2018a; Dudin and Lyasnikov 2018).

Crimeware-as-a-service

Crimeware-as-a-service is one of the most advanced types of cybercrime whereby a buyer finds a vendor who arranges and conducts the actual crime. For example, with malware-as-a-service, a buyer can indicate a number of launches, timeframe, and other specifics (Positive Technologies 2018b). To increase their profits, malware coders have started distributing instances of their software via a partnership programme. A buyer gets the malware code and distributes it, while the coder gets the usage statistics and paid ransoms. The coder usually keeps 15 to 50% of the ransom, and the distributor gets the remainder. However, the existing research does not indicate how these transactions take place. This scheme has been applied in the distribution of Gandcrab, Tantalus, Aleta, Princess, Rapid, Scarab, Sphinx, Lovecraft, and Onyonlock (Positive Technologies 2018b). The Exobot trojan, before it was anonymously leaked online in May 2018, could be rented for 750 USD per one week’s use or 2,400 USD per month (BI.ZONE 2019).

Reports show that demand for malware production outstrips supply threefold on dark web markets, while demand for malware circulation outstrips supply twofold (Positive Technologies 2018b). First, this indicates that cybercriminals want to invest in new tools and programmes (Group-IB 2018a). Second, partnership programmes where malware or other services can be used by multiple groups are becoming more common. This development presents a number of problems for investigators: without unique programmes and codes, it is difficult to attribute an incident to any particular group (Positive Technologies 2018b; Bi.ZONE 2019). In some cases, malware developers publish the source code of their programs online and on their own initiative[51], a tendency which industry experts expect to continue (Group-IB 2017).

Fraud and Theft

Social engineering

Social engineering is a manipulative method of gaining victim's trust and finding out their personal and bank information which often results in a victim initiating money transfers. Criminals contact victims via all available channels, including phone calls, email, messengers, texts, and even regular mail (Verevkin and Verevkin 2017). Offenders often use IP telephony (Session Initiation Protocol) that spoofs the incoming call to look like a real bank's phone number (starting with 8-800). Social engineering has become the main vector of attack when stealing money from individuals. In Russia, this vector accounts for 80% of attacks on all bank customers (BI.ZONE 2019).

Criminals often introduce themselves as bank representatives and encourage their victims to reveal their personal information, bank card number, one-time passwords for 2FA sent via SMS, card expiration date, CVV2/CVC2 codes, and other information. Sometimes, criminals 'inform' their victims that their cards have been blocked or frozen and ask for card details to 'verify' the identity. Another scheme includes criminals telling victims that their relatives/ friends have had an accident and need financial support. In some cases, offenders still attempt 419-type/advance fee scams, telling victims that they have won a lottery or a prize and are asked to share their bank card details to pay a tax on the prize (Sharova 2017). Until mid-2018, criminals preferred to contact their victims via SMS, but by the end of the year they almost completely switched to phoning (BI.ZONE 2019).

The popularity of social engineering attacks does not seem to be decreasing. In August 2019, an editor of a Russian online media outlet *TJournal* wrote about 'a new wave' of bank fraud conducted via phone which he had experienced personally (Kamaletdinov 2019). Big Russian banks, Sberbank and VTB, along with the journalist's bank, Roketbank, confirmed an increase in criminal activity of this kind in the summer of 2019. While banks know about social engineering attacks, the literature suggests that they might not give it a high priority for two reasons (Group-IB 2017): first, this type of fraud does not amount to big losses per operation for a bank; second, it is almost impossible to retrieve the stolen money because the clients gave away their private details willingly.

Russian banks and regulators usually suggest that victims of social engineering have poor technical and financial skills (Bank of Russia 2019), placing the onus on the consumer to not be victimised. However, efficient and prepared callers can manipulate even people with good knowledge of technology, social media and trends into revealing bank information to a stranger on the phone.[52] Moreover, the 1992 Consumer Rights Protection law does not explicitly cover operations and services in the financial field, making legal disputes equally challenging for clients and banks. The Association of Russian Banks has proposed adopting a new law specifically for consumers of financial services, but there have been no changes yet (Koshkina 2017). Nevertheless, the Central Bank tries to increase clients' data protection. In May 2018, the regulator amended the provision 'On information security requirements' stating that banks will have to use strictly certified software for handling transactions, as well as conduct penetration testing every year and inform the Central Bank of incidents (BI.ZONE 2018).

Phishing

Phishing is a very popular tactic for criminals and more people are attacked through phishing than with banking trojans and other malware. There are a couple of dozen groups in Russia that use phishing to attack financial institutions and the number is increasing due to the growing supply of automated services which simplify work for criminals thereby attracting more of them (Group-IB 2017).

In phishing attacks, criminals may obtain sensitive information, such as usernames, passwords, and bank card details, by disguising an online page as a trustworthy entity that then redirects users via special links. Alternatively, cybercriminals entice victims to visit phishing websites by targeting them with Google AdWords (Holub and O'Connor 2018). Every day, around 950 people become phishing victims in Russia and the Commonwealth of Independent States (Group-IB 2017). The average amount stolen is 15-16 USD. Overall, losses from H2 2017 to H1 2018 were estimated to be 3.1 million USD (Group-IB 2018a), a decrease from the 4 million USD estimated annual loss of the preceding year. This decrease appears to be a direct result of the 2017 arrest of the owners of two Russian Android botnets used for phishing attacks (Cron and Tiny.z).

Out of thousands of potential victims that visit phishing websites, approximately 10 to 15% enter their bank card data (Group-IB 2017; 2018a). Some researchers suggest that the high rate of this crime can be explained by poor technical skills of the users (Kaznova and Ovchinnikova 2017). In 2018, BI.ZONE conducted an experiment, where they sent more than 300,000 emails to employees at financial organisations, and found that about 16% of the recipients followed the link in the message, while 7% entered their corporate credentials on a phishing site or opened a malicious attachment (BI.ZONE 2019).

While most banks use adequate anti-phishing tools, employees often check their personal email, which is not protected by corporate security tools, on their work computers. Accordingly, attackers collect personal email addresses of a wide range of bank employees and send them emails with malicious attachments during business hours. Apart from individual targets, email phishing remains the key infection vector for initial penetration into the networks of financial institutions and a first step in carrying out complex cyber-attacks (Group-IB 2017; Solar JSOC 2018).

Phishing was successfully used by the Cobalt group to steal 400 million rubles (6 million USD) from the Soyuz bank. After one of the bank employees opened a phishing email, hackers accessed the processing system and changed debit cards settings to having no withdrawal limits. Subsequently, the attackers used the cards to withdraw money from other banks’ ATMs (Goryacheva 2018). Phishing and malware are also the main threats for investors working with cryptocurrencies. Hacked cryptocurrency trading platforms generated 882 million USD for criminals worldwide in H2 2017 – H1 2018 (Group-IB 2018a).

Online and Mobile Banking

An analysis undertaken by Positive Technologies shows that, as of 2019, every single online banking system on the Russian market that they researched had vulnerabilities that can lead to serious consequences, while 54% of banking apps had vulnerabilities that hackers can exploit for theft and fraudulent operations. Therefore, criminals will likely continue to develop new malware and target mobile banking systems in Russia (Positive Technologies 2019).

Russian-speaking hackers create, on average, one to two new malicious programmes per month designed for committing theft of funds. Out of 22 of such programmes found on the dark net by Group-IB, 20 (91%) were created and are controlled by Russian speakers (Group-IB 2017).

Group-IB (2017; 2018a) outlined the six most common types of theft from bank clients:

- Theft through SMS-banking;
- Card-to-card transfers;
- Online-bank transfers;
- Gaining access to mobile banking;
- Counterfeit mobile banking; and
- Purchases via Apple Pay.

The Central Bank of Russia estimated that cybercriminals stole more than 1 billion rubles (15.1 million USD) from individuals’ bank accounts in 2017 (FinCERT Bank of Russia 2018), but the actual numbers may be higher, especially if we look at types of criminal activities separately. In 2018, the average amount stolen from bank cards was 3,320 rubles (50 USD) per theft, a 9.6% increase compared to 2017 (Central Bank of Russia 2019). The majority of unsanctioned operations with bank cards are the card not present (CNP) operations. In 2018, more than 80% of all card operations were CNP operations. In 2018, the estimated losses from illegal CNP were 1.077 billion rubles (16.3 million USD) (Central Bank of Russia 2019). Russia’ inter-bank payment system SPFS, Russian: Система передачи финансовых сообщений, a Russian system developed to operate instead of SWIFT, has been successfully breached, with $920,000 USD taken in July 2018 (Moiseienko and Kraft 2018).

To succeed in these operations, criminals require certain malware, and trojan programmes in particular. Once a trojan is entrenched in the device's system, it locates an internet banking app, a hotel booking service, or a messaging service (BI.ZONE 2019). A trojan can also help a criminal to establish control over a device and to get the victim’s banking and personal details. For example, the Agent.SX, Flexnet, Granzy, and Agent.BID trojans proved to be successful in compromising SMS-banking on Android devices. In 2017, at least 12 new banking trojans for Android appeared on the market. Criminals choose to target Android devices because it is easier to compromise them than iOS devices and because most users in Russia access mobile applications on the Android platform (68%) (BI.ZONE 2019).

Cybercriminals prefer to launch large-scale trojan attacks because they are simple to perform and the sums of money stolen per victim are relatively small. Each malware programme infects an average of 7,400 mobile devices a week (BI.ZONE 2019). In 2017, clients in Russia and CIS lost 13.6 million USD because of banking trojans on Android (Group-IB 2017).

Android phones have also been exploited with the help of iPhones (Group-IB 2017). Offenders get bank card details from the mobile apps on infected Android phones and then link these details to Apple Pay on their iPhones using SMS-2FA confirmations intercepted with the trojan. Thus, the attackers have a fully functioning Apple Pay service linked to a victim’s bank account. With Apple Pay, if the user confirms the payment by his/her fingerprint during the payment process, the transaction must be executed, making it difficult to stop such fraud. A PIN-code may be required for large-sum purchases, but some banks have a list of authorised venues where PIN-codes are not requested even for expensive purchases which allows fraudsters to choose these specific locations (Group-IB 2017).

The market for PC banking trojans in Russia has changed significantly in the last two years. While in 2017, experts detected six new PC trojans targeting users, in 2018, PC trojans left the malware market completely (Group-IB 2017; 2018a). By 2018, no criminal groups in Russia used PC trojans for theft from individual users. Moreover, only three known groups, Buhtrap2, RTM, and Toplel, applied this method to target companies. However, outside Russia, experts noted that six new PC trojans entered the market in 2018: IcedID, BackSwap, DanaBot, MnuBot, Osiris, and Xbot (Group-IB 2018a).

Data Theft for Profit

Positive Technologies experts observed a noticeable share of attacks on financial institutions that only aimed at stealing personal and card data of the clients that could be sold later on the dark web (Positive Technologies 2018a). Offenders can steal or buy sensitive information and documents from organisations, including all of the credentials associated with a company’s various bank accounts (account numbers, logins, passwords, and tokens) (SecureWorks 2016). If the company has good credit, criminals may apply for bank loans, high-limit credit cards, car loans, and other lines of credit using the stolen data.

Experts who work with victim banks have noticed that data theft is often a low priority for those banks because it comes with lower reputational risks compared to thefts via banking transfers or ATMs, because successful attacks on these targets are widely covered by the media (Group-IB 2017). Industry experts predict that criminals may prioritise data theft and destroying banks’ IT infrastructure over money theft in the future (Group-IB 2017; Positive Technologies 2018c). To that end, criminals are most likely aware of banks' security priorities and will increasingly exploit low-priority targets. For instance, in August 2019, the Russian business newspaper *Kommersant* reported that the personal data of 70,000 Binbank clients had been leaked and were on sale on online black markets for five rubles per person (0,077 USD). The attack may have happened because the provisional administration from the Central Bank of Russia did not monitor Binbank information security problems – and criminals exploited this oversight (Goryacheva and Trifonov 2019).

Ransom and Extortion

Criminals who seek to extort can use different methods and may target both individuals and companies. Most common extortion methods include infecting devices with malicious ransom programmes and initiating DDoS attacks on a victim's website or service. When extorting, attackers usually block victims from gaining access to their devices, files, social media accounts, or systems related to business. To restore access, attackers demand a remittance in both fiat and virtual currencies. Encryption-based ransomware is now used both by independent hacker groups and state sponsored cybercriminals (Group-IB 2017). In some cases, disruption and extortion attacks are used by cybercriminals to cover their tracks and distract attention from high-profile targeted attacks.

Ransomware use attracts criminals because mass attacks generate big profits that easily make up for the cost of the malware, which averages 270 USD on the dark web (Positive Technologies 2018b). With the ransom rate usually set at 200-500 USD (usually paid in cryptocurrency), combined damage from WannaCry, NotPeyta, BadRabbit, Locky, and Cerber campaigns was estimated to be around 1.5 billion USD. Locky and Cerber ransomware were reportedly distributed through a partner programme by Russian-speaking hackers (Group-IB 2017).

Large-scale ransomware attacks often bypass Russia. Advanced Persistent Threats that operate out of Russia have a history of targeting political adversaries of the Russian state (Mandiant 2017). For example, massive 2017 attacks by WannaCry and NotPetya[53] caused little to no damage to Russian companies; the same was true for GandCrab. GandCrab checked keyboard language layouts to avoid infecting potential Russians (Kujawa et al. 2018). NotPetya, however, targeted Ukrainian legal and state entities (Group-IB 2017). The subsequent large-scale ransomware to target Ukraine and Russia was BadRabbit. It targeted the Ukrainian subway system, state organisations, and an airport, as well as state media companies in Russia (Group-IB 2018a). Experts found that BadRabbit's code consisted of parts of NotPetya's source code with some upgrades, in particular in the ransom payment process (in bitcoin). NotPetya had only one wallet for all victims for transferring the ransom which suggests that the criminals did not plan to recover the victims' files but were prioritising a disruption of services. On the other hand, BadRabbit designed an automated generation of a unique key to every computer and a creation of a new wallet for every key (Group-IB 2018a).

Another popular ransomware tactic is to target social media pages for ransom or blackmail. For example, a group in Ukraine gained access to Instagram accounts and demanded a ransom between 350 and 1,000 USD from their victims, including those based in Russia (Dolgieva 2018a). Often, blackmailed victims want to avoid any publicity and do not contact the police or cybersecurity experts which makes it difficult to obtain accurate statistics. However, at least 5% of all attacks on users is aimed at blackmailing them with stolen data from social media pages, personal devices, and Cloud storages (BI.ZONE 2019). Another scheme involves criminals gaining control over someone's VK[54] page and sending messages to the victim's friends asking for money under a certain pretext. Some users who do not know that their friend's account has been hacked send money to the criminals.

Extortionists can also organise DDoS attacks[55]; on the dark web where the competition can be high, most Russian hackers who offer DDoS attack services are willing to perform a free 5- to 10-minute DDoS test for customers (SecureWorks 2016). However, overall, DDoS attacks are one of the least popular cybercriminal methods and make up only 3% of all cyber-attacks in Russia (Positive Technologies 2018c). The most DDoS targeted industry is the gaming industry with 64% of all registered attacks. Experts suggest that with further development of cybersport, this industry will continue to attract criminals. E-commerce comes second, with 16% of attacks (Rostelecom 2019).

While the average DDoS attack lasts around two hours, Rostelecom reported that the longest attack of 2018 in Russia lasted 280 hours (11 days and 16 hours). The attacks are becoming more powerful within Russia: in 2017 the record was 54 Gbit/sec, and in 2018 it was already 450 Gbit/sec. However, that is far below the world record of 1.7 terabit/sec detected in 2018 outside Russia (Positive Technologies 2018c). Low costs of DDoS attacks result in a significant increase in this type of attack over time; in 2018 the growth was twofold (Rostelecom 2019).

DDoS attacks can also be used as a diversion tactic while criminals are stealing money from bank clients. During the attack, bank clients cannot access their accounts immediately due to the overloaded servers. Thus, while the bank is trying to fight the DDoS attack, clients may not be able to report theft (Kupriyanov and Krashennikov 2018).

Cryptojacking

Secret mining, or cryptojacking, is an unauthorised use of someone else's computer to mine cryptocurrency. To begin cryptojacking, criminals need to obtain malware. On the dark web, 20% of all malware offers in 2017 were for cryptojacking (Positive Technologies 2018b).

Cryptojacking presents a threat because it is not immediately clear that a computer or another device is being used by criminals. To recognise that a computer is engaged in secret mining, security specialists need to pay attention to such signs as energy blocs overheating, decreasing battery life, and increased power usage (Kondrashin 2018; Group-IB 2018a).

Security experts in Russia reported a few incidents of cryptojacking in the past two years, including one where a criminal had a botnet of around 5,000 servers for cryptojacking and was earning 200,000 rubles (18,000 USD) a month by mining cryptocurrency (Positive Technologies 2018a). Sometimes employees secretly use work computers and servers to mine cryptocurrency because at work they have access to many powerful computers at once. Such were the cases of a system administrator working for Moscow’s Vnukovo airport who was mining cryptocurrency using servers at work; a Transfent oil company employee mining Monero cryptocurrency; and a mining employee of Rosatom state nuclear energy company (Dolgieva 2018c).

In Russian banks, mining software is usually detected in employees’ work computers where it is installed via malware, while outside the financial sector, mining software is secretly installed by the information security specialists in 30% of cases (Solar JSOC 2017b). However, with the price of bitcoin falling and mining becoming more difficult, secret mining decreased in 2018 (Positive Technologies 2018c). In the first quarter of 2019, 23% of malware[56] was used for cryptojacking, while in the last quarter it was only 9%.

Cybercrime Proceeds and Their Currency Properties

Fiat and Virtual Currencies

Fiat currencies are currencies that are issued and backed by sovereign states. For Russia, the fiat currency is the Russian ruble. There are different types of transactions involving fiat currencies, with varying degrees of transparency, traceability, and security. Russia has AML/TF regulations in place that focus on fiat currencies.

Fiat currencies are used in cash payments, payment cards (i.e. Visa; MasterCard; Mir (Russian: Мир), the Russian National Card Payment system), bank transfers (i.e. SWIFT and SPFS, the Russian equivalent of the SWIFT system), and money transferring businesses (i.e. Western Union).

Electronic payment systems in Russia operate with digital fiat currencies. In Russia, the three most popular e-payment systems are Yandex.Money, WebMoney, and QIWI. Transfers with these payment systems can be less transparent because some e-wallets allow their users to remain anonymous and use the services without ID verification.

YandexMoney («Яндекс.Деньги») is an e-payment system which is co-owned by Russia's leading search engine Yandex and Russia's largest bank Sberbank. This partnership allows users to top up their e-wallets through the chain of Sberbank’s ATMs and online banking. YandexMoney is also partners with MasterCard and provides both virtual and physical payment cards which can be linked to ApplePay and SamsungPay. There are over 46 million registered e-wallets on the platform[57]. In 2017, 33% of all Russian internet users used YandexMoney, while in 2018, the percentage rose to 48.5%. It is possible to open an anonymous e-wallet in order to send and receive small amounts of money via the platform.

WebMoney is not legally registered as an e-payment system even though it technically operates as such. The system uses special currency units that are equivalent to the corresponding fiat currency, and one e-wallet can operate with only one currency unit. However, users can open any number of wallets. For example, WMR is an equivalent of the Russian ruble in R-wallets; WME is an equivalent of the Euro in E-wallets; and WMZ is the equivalent of the US Dollar in Z-wallets, and so on. According to its website, there are 39.5 million registered users, of which 883,000 users were active in August 2019. On average, WebMoney users perform 200,00 operations every day.[58] In 2019, WebMoney joined Sberbank’s instant transfer ecosystem where clients can make instant transfers from Sberbank cards to WebMoney wallets and vice versa. To make the transfer, clients only need to know the recipient's phone number, which the card or wallet is linked to.

QIWI is an e-payment service provider with 20.3 million active e-wallets and 90,000 payment kiosks around the country[59]. QIWI has a partnership with VISA under the VISA QIWI Wallet brand. With the QIWI card, clients can pay offline and online. As with other e-payment services, QIWI wallets are linked to mobile phone numbers, and, to make a transfer, users only need to know a phone number.

With e-wallets from any of these three e-payment systems, users can make and receive transfers, as well as pay for mobile phones, television, utilities, fines, mortgages, and so on. To access an e-wallet, one usually has an ID number and a password (Sharova 2017, Nemova 2018). There are different ways to top up an e-wallet; at least two of them allow some anonymity: cash top-up at the automated kiosks and transfers from a phone number balance. Other ways include online banking and bank transfers. We discuss the e-payment opportunities for criminals further in the *Non-traditional transactors* section.

Virtual currency is a digital currency built with cryptographic protocols. The most commonly traded cryptocurrency is bitcoin. There are services and crypto ATMs that exchange cryptocurrencies for and to fiat currencies. Cryptocurrencies and operations with them are a grey area in Russia. As a result, operations with cryptocurrencies, including mining, are not taxed due to the lack of legislation. In 2014, the government considered banning cryptocurrencies due to the many potential risks that come with anonymous transactions and decentralised emission. In 2014 through 2016, Roskomnadzor, Russia's main communications agency, blocked a few websites devoted to cryptocurrencies and blockchain (Povetkina and Ledneva 2018). As of August 2019, the State Duma is still reviewing a bill on cryptocurrencies and their regulation (Duma.gov.ru 2018). At the same time, a vast majority of judges, prosecution officers, Investigative Committee and Ministry of Interior officers believe that existing Criminal Code norms do not cover all illicit activities with cryptocurrencies (Dolgieva 2018b).

Criminal use of cryptocurrencies can be divided into two general groups. In the first group, cryptocurrencies serve as a means of buying tools for cyber-attacks, drugs, weapons, and money laundering. In the second, cryptocurrencies are stolen as part of cybercrime, such as extorting people with ransomware or hacking crypto wallets and cryptocurrency trading platforms (Sidorenko 2016). While cryptocurrencies are not illegal tender in Russia, operations with them may be checked for money laundering or financing terrorism (Rosfinmonitoring 2014). However, research shows that law enforcement may have little to no knowledge of operations with cryptocurrencies which can in turn complicate investigations where cryptocurrencies are involved (Korchagin 2016; Dolgieva 2018b; Lavronenko 2018c). On the other hand, even if such investigations are completed, legal regulations do not cover cryptocurrencies so that criminals may exploit these gaps (Sidorenko 2017; Sidorenko 2018). Finally, in drug related crimes, Russian investigators might not even look for crypto wallets because investigators might not know what crypto wallets are (Dolgieva 2018d).

Nevertheless, Russian authorities try to regulate cryptocurrency flow in the country. In August 2018, at least 25 crypto ATMs in 6 Russian cities were seized at the request of the Central Bank and Public Prosecution Service (RIA Novosti 2018). All of the ATMs belonged to BBFpro. As of August 2019, there were 59 legally registered crypto ATMs in the country where anyone can buy bitcoin, with 9 ATMs in Novosibirsk, 7 Rostov-on-Don, and 5 in Moscow (Coin ATM Radar 2019).

The Russian financial intelligence unit Rosfinmonitoring (2017) reported that drug dealers increasingly used cryptocurrencies – particularly Bitcoin – to pay drug traffickers and to launder money; no information in terms of the payment and laundering processes, however, was reported. Such offences have been registered almost in all Russian federal districts. Although no statistical data are available to indicate what percentage of drug crimes involve cryptocurrencies, there are at least 86 known cases from 2015 to 2017 in Russia where cryptocurrencies were used in drug deals; however, in no drug related cases was cryptocurrency actually confiscated (Dolgieva 2018d). On now closed RAMP, Russia’s largest drug marketplace, customers paid into either a bitcoin or QIWI account, meaning that sellers also accumulated their proceeds in bitcoin (Shubin 2018).

Apart from fiat and virtual currencies, other digital assets exist, for instance the ones cultivated in videogames and used in social media. On VK, Russia’s biggest social media platform, for fiat currency, users can buy ‘votes’ (голоса), which, in turn, act as VK currency for purchasing paid features on VK apps, as well as gifts for other users and stickers. VK votes can attract fraudsters primarily as a means to steal personal information or to acquire access to the user’s page. This scheme is aimed at users who would like to increase their VK votes balance for popularity reasons; therefore, offenders may offer free votes or promise to multiply them. In return, they may ask for personal information, including a password from the VK page, or they may ask their victim to complete tasks and to download programmes (which most likely contain malware) (VK n/d).

Proceeds of Cybercrime

Cybercriminal operations in Russia are a multimillion-dollar industry. Yearly profits are estimated to be between 50 and 100 million USD on the Russian market alone; however, industry experts report that Russia-based hackers earn the majority of their profits outside Russia (Group-IB 2017; Group-IB 2018a). This finding supports our earlier arguments that hackers do not focus on one market or country but target any region that offers an opportunity.

Phishing may seem to cause little damage for banks, but the number of victims amounts to hundreds daily in Russia. Group-IB estimated profits from phishing over a period of 12 months to be around 4 million USD (Group-IB 2017; 2018a).

Stealing personal data is another source of profit for criminals, albeit less instant than phishing because the stolen data are then used for blackmail, money theft, and sale on the dark web (Positive Technologies 2018a; BI.ZONE 2019). In 2016, estimates for combined sellers' earnings were around 1 million USD for smaller lots and 2 million USD for larger lots of stolen personal information on international markets (Holt, Smirnova, and Chua 2016). While this appears to be a profitable venture for data sellers, data buyers could earn substantially more by using the acquired data in theft and fraud.

The price of personal data on internal Russian markets is likely to be lower than the international average. For instance, the business newspaper *Kommersant* reported that the personal data in a database of 70,000 Binbank clients costs around 5 rubles per person (0.077 USD) (Goryacheva and Trifonov 2019). The market in Russia for stolen bank card information (text data) amounts to 95 million USD, and electronic card copies amount to 567 million USD (Group-IB 2018a).

In the fiscal year of 2016-2017, although attacks on individuals were on the rise, industry experts reported a significant decrease in the amount of profits resulting from stealing from companies. During this same time, successful targeted attacks on Russian and CIS banks amounted to 27 million USD stolen, while 10 more million USD were stolen from companies by using malware in online banking systems (Group-IB 2017). During the following fiscal year (2017-2018), targeted attacks on banks brought criminals only 21 million USD (Group-IB 2018a); this decrease can be linked to the arrest of the leader of the Cobalt cybergroup (Goryacheva 2018).

In the biggest publicly disclosed cyber-attack on Russian banks in 2018, criminals managed to steal 58 million rubles (870,000 USD) (BI.ZONE 2019). The offenders had infiltrated the PIR bank’s internal infrastructure through a phishing email and gained access to its automated workstation of the Central Bank of Russia client, thus stealing from PIR's corporate account at the Central Bank.

The Central Bank’s FinCERT presented different statistics of overall losses to theft. According to them, from January to August 2018, banks lost to criminals in overall 20 cyber-attacks only 76.5 million rubles (1.1 million USD) (Positive Technologies 2018). In both individual and corporate losses, it appears that data from security companies and state regulators may differ with the latter sometimes reporting smaller amounts of losses.

Transactional Facilitators

Cybercriminals use a variety of strategies to facilitate the transaction of the proceeds of their crimes and to buy products and services. The literature highlights the use of money mules, banks and other financial bodies, and e-payment services.

Money Mules

Money mules are people who are involved in transferring money for someone else in person, electronically or any other way. Normally, mules get a small part of the money for their services. Criminals can find mules in various places, including the dark web where 10% of all sellers reportedly offer cashing out services and 35% offer facilitating transfers via e-payment systems (Positive Technologies 2018b). The literature on how money mules are hired and rewarded by Russian speaking groups, as well as where they come from or what happens after the cash-out, is very scarce.

Cash withdrawal can be one of the most challenging stages of financially motivated cybercrime; consequently, money mules are constantly looking for new schemes. One method focuses on the use of mules, both domestic and foreign, asking individuals to facilitate onward transfers of stolen money in exchange for a small commission (Soudijn and Zegers 2012; Mikhaylov and Frank 2016). Another method involves a card processing scheme tested in Russia and then used in the countries of the former USSR and the United States by all major cybercriminal groups (Group-IB 2017). First, attackers open or buy around 30 cards of the bank whose IT system they compromised and then give the cards to the mules who take the compromised cards abroad. Next, the criminals connect to the card processing system and remove or increase cash withdrawal limits for the compromised cards held by the mules. Attackers may also remove overdraft limits which makes it possible to overdraw accounts with the compromised debit cards. Finally, the mules withdraw cash from ATMs. There is no indication as to what happens to the money once it is withdrawn from the ATMs. The average theft by this method is an estimated 500,000 USD (Group-IB 2017).

Mules can travel to multiple countries to cover their tracks. In the attack on Dutch-Bangla bank in Bangladesh, the Russian speaking Silence group[60] hired at least seven Ukrainian citizens to withdraw cash from the bank's ATMs in Dhaka. The mules reportedly came to Bangladesh from Turkey, and from Bangladesh they planned to fly to India, but six of them were arrested due to CCTV footage (Group-IB 2019).

Large-scale theft operations can involve dozens of mules, as in the case of the Russian bank Kuznetsky. In August 2015, using MasterCard bank cards issued by Kuznetsky, fraudsters dispensed 470 million rubles (7.1 million USD) from the ATMs of other banks. They hacked the UCS[61] processing system configuration, which incorrectly handled rolled back transactions so that the criminals' account balances were restored after every withdrawal. The fraudsters must have emptied more than 200 ATMs with 3,000 operations within a day which would not be possible if it had not been a large group (Eremina 2016).

There is little information in the reviewed literature on what happens to the stolen money which has not been cashed out. Only BI.ZONE (2019) outlines the main destinations where the money is transferred:

- Dummy cards (63%);
- Immediate online purchases (digital products, stocks, music record shops, dating sites, and retail goods) (17%);
- Mobile phone accounts (8%);
- Bank accounts (4%);
- E-wallets (3%).

Research shows that few Russia-based criminals cash out their proceeds. Group-IB experts estimated that criminals cashed one third of all stolen money, or 23 million USD, in H2 2016 – H1 2017 and only 15 million USD the next year (Group-IB 2017; Group-IB 2018a). However, BI.ZONE reports that cybercriminals use ATMs and local branches to withdraw stolen cash in Russia in only 5% of cases (BI.ZONE 2019). Most cashing out takes place in Moscow (16%), St. Petersburg (11%), and Chelyabinsk (6%).

At the same time, the Central Bank of Russia reported a threefold increase in money outflow from Russia in 2018[62] (26.5 billion USD) compared to 2017 (9.6 billion USD) (Anapolskaya and Dvoretsky 2019). While not all of this money is illegal proceeds of crime, it is possible to suggest that criminals may prefer to keep their profits outside Russia or to cash them out outside the jurisdiction in which they operate to diminish risks of being investigated. This argument is supported by Group-IB (2017) who reported that withdrawing stolen money in another country can be appealing because the bank's security service cannot promptly contact the local police nor get video records from surveillance cameras, making it more difficult to arrest the perpetrators.

Banks and other financial bodies

Cybercriminals have used banks and other financial organisations to facilitate transfers for various purposes, including laundering transactions. This is typically achieved by using stolen data to open bank accounts, issue cards in the name of real bank clients without their knowledge, use national and international e-payment systems or e-wallets under someone else's name, accept fake legal entities making transfers, and organise a chain of financial operations via multiple bank accounts (Kalashnikova and Arkhipov 2018; Lavronenko 2018b; Positive Technologies 2018b). Most dummy cards that are used for transferring the proceeds of cybercrime are issued in Moscow (16%) and St. Petersburg (6%). Among other cities, Chelyabinsk leads with 5% of dummy cards issued. However, there are no details on the banks and services involved (BI.ZONE 2019).

Non-traditional Transactions: E-payment services

Criminal priority to stay anonymous also encourages hackers to use services from non-traditional transactors. Here, we include e-payment services in Russia that provide electronic online payments with or without linked bank accounts. They are PayPal, which is a global presence, and Yandex.Money, WebMoney, QIWI, and VK Pay which are widely used in Russia. QIWI also operates in Kazakhstan, Belarus, Moldova, Romania, the United States, Brazil, Jordan, and in nine more countries via a franchising agreement.

To set up an e-wallet on YandexMoney, a user needs a unique login name, a password, and a mobile phone number[63]. A payment account number is automatically created when a wallet is set up. The phone number is used to verify the account and operations with it via SMS texts. After the initial set-up, YandexMoney asks users to link a bank card to the wallet, but they can skip this step and use the wallet anonymously.

The process of setting up e-wallets on WebMoney and QIWI[64] is similar to YandexMoney. Users create an account with a mobile phone number which is then used for 2FA. All three systems offer upgrading basic anonymous accounts by adding personal data such as full name, date of birth, and passport details. Accounts with minimal restrictions require an in-person ID verification at the specialised offices.

E-payment systems appeal to Russian criminals for two main reasons (Kaznova and Ovchinnikova 2017). First, it is possible – and common – to have an anonymous, albeit low-volume, e-wallet: the maximum balance cannot exceed 15,000 rubles (226 USD) and all operations with the account cannot exceed 40,000 rubles a month (603 USD).[65] It estimated that around 10 million people in Russia are using anonymous e-wallets (Chernyshova 2019). Since WebMoney is not a registered e-payment system, it has different limits for anonymous users: 45,000 WMR (equivalent of the Russian ruble) for the account balance, and 90,000 WMR for total operations per month[66].

Second, due to the balance restrictions imposed by all e-payment systems in Russia, criminals may choose to open hundreds and even thousands of e-wallets. In one case in the Siberian Federal District, more than 2,000 e-wallets totalling 1.2 billion rubles (18 million USD) were discovered in a drug trafficking operation (Rosfinmonitoring 2017). When RAMP was operational, between 50% to 70% of all payments were made into QIWI wallets; the rest went into a bitcoin account (Persianinov 2017).

E-wallets can appeal to criminals especially if they have a facilitator inside the e-payment system. Even though Rosfinmonitoring tries to monitor how e-payment systems verify users’ identities to prevent illicit transactions, insider facilitators can approve user verification in those systems for criminals (Positive Technologies 2018b).

However, Russian authorities are now trying to combat the anonymity of e-payment systems. At the end of July 2019, the Russian Federal Council approved changes initiated by Rosfinmonitoring to the law on payment systems, thereby banning anonymous top-ups of e-wallets with cash. When the changes take effect, it will be possible to top-up an e-wallet only with a bank account (Chernyshova 2019).

QIWI-wallets can also be used for transferring rubles after a bitcoin exchange. Criminals can then transfer funds from a QIWI-wallet to a bank account of a third individual (such as a mule). These and other multi-step schemes make investigating money origin complicated for law enforcement (Vasyukov and Bulyzhkin 2017; Alexandrov 2018; Kumukov 2018).

VK Pay presents another platform for alternative transactions in Russian rubles, based on card-to-card operations and performed in the VK messenger. The maximum transaction can be 75,000 rubles (1,142 USD). Launched in 2016, the service estimated the size of the potential audience for VK Pay transfers at 60 million users. As of 2019, 15.4% of users who have made a purchase online in the past year used VK Pay (Sedlov 2016; Mediascope 2019). While we have not found any substantial research on criminal use of VK Pay, there are certainly ways to exploit this service for illegal transactions. One of them is social engineering: users can be manipulated into sending money to an unknown person on VK; due to its specifics, the victim does not need to know the fraudster’s card number. Additionally, users can pay for services and goods without paying tax.

Regulations vis-à-vis Cybercrime

Legal Regulations

Most cybercrime in Russia falls under the Criminal Code’s Chapter 28 (Articles 272, 273, 274), which covers access to computer information, data theft and fraud in the field of computer information. Punishment for these crimes varies from fines, community service and imprisonment up to 7 years. This legislation has not been changed significantly since its adoption in 1996 and is considered largely outdated (Veprev and Nesterovich 2018). Even basic cybercrime terminology is debated in Russia. While current legislation uses the term ‘computer information’ to cover cybercrimes, experts propose updating the wording and including terms like ‘high-tech crimes’, ‘digital information’, and ‘electronic information’ (Arzamastsev 2017).

Money laundering and financing of terrorism are mostly covered in the Federal Law 115 and Article 174 of the Criminal Code (Shokhin 2018). Money theft from bank accounts and e-wallets, even with previously obtained personal data, is prosecuted according to Article 159.6 of the Criminal Code (*‘Fraud in the field of computer information’*) or Article 158 (*Theft*) (Nikulina 2015; Sharova 2017; Lebedeva 2018a; Lebedeva 2018b).

Many researchers point to a growing gap between technological and digital developments and current legislation in Russia (Verevkin and Verevkin 2017). For example, qualifying phishing as a crime in Russia presents many legal challenges. While the Supreme Court of Russia says that phishing may be prosecuted as theft, some scholars argue that the object of theft has to be part of the material world, and personal data is not considered to be such. Thus, other Criminal Code articles, such as Fraud in the Computer Information Field (Article 159.6), Illegal Accessing of Computer Information (Article 272), and Violation of Rules for the Operation of Computers, Computer Systems, or Their Networks (Article 274), should be considered by the courts (Dolgieva 2018a). Additionally, the Russian Criminal Code does not cover practices of illegal cashing out; consequently, such crimes are usually prosecuted as theft (Loshkarev 2016).

Another point to consider is Russian criminals operating at an international level. With no criminal extradition relationship with the United States and mixed extradition results with the European Union, Russian hackers may target businesses in any of these nations with minimal risk of arrest (Smirnova and Holt 2017).

Law enforcement agencies start their investigations of cybercrime resulting in money theft after an individual victim or financial organisation reports a crime. Some researchers suggest that banks can be reluctant to report such crimes because of reputational risks and lengthy legal investigations[67] (Linnikov 2017). Also, individuals may not report small-scale thefts which means financial cybercrimes in Russia are likely to be significantly underestimated.

Police can rarely identify suspects straight away; at best, police can establish only the IP-address and internet provider. If the police manage to seize a computer that was used by criminals, a preliminary investigation can take one or two months (Timofeev 2016). Regarding financial operations, law enforcement can contact Rosfinmonitoring; however, some suggest that this communication needs to be greatly improved (Izutina 2018).

When it comes to phishing, it is necessary for regulators to block phishing websites in a timely manner (Group-IB 2017; Group-IB 2018a). Reporting and investigating such websites are done by internet providers, security companies, and now FSB Russia. As a result, hundreds of domains are blocked every month (Shestoperov and Moiseyev 2019).

What cyber offenders do with the profits of their crimes is difficult to investigate due to the latency of cybercrime in general (Lavronenko 2018b). Some experts argue that only around 10% of all reported cases are investigated, and even fewer cases actually go to court (Batukhtin 2018). Other experts suggest that the number of open cases represents less than 1% of all committed cybercrimes (Filimnov 2014). Law enforcement's low level of expertise regarding cybercrime and money laundering schemes, including cashing out operations, along with bank employees' lack of training in identifying suspicious operations only compound Russia's investigative woes (Linnikov 2017; Dulskaya 2018; Izutina 2018; Lavronenko 2018a).

Financial Regulations

Rosfinmonitoring, Russia's main financial intelligence unit, has a number of national risk assessment goals, which include identifying the most common money laundering schemes, detecting gaps in the national AML/CFT system, and promoting a common understanding of ML/TF risks among all AML/CFT system participants. The regulator also oversees the exchange of information for relevant stakeholders in the field (Rosfinmonitoring 2017).

Despite the high number of companies exchanging information with the regulator, some researchers point out the ineffectiveness and impracticality of the daily messages and reports sent by companies (Mikhailova 2019). Scholars also suggest that criminals arrange their deals and operations in such a way as to avoid being reported to Rosfinmonitoring altogether. Similarly, the International Monetary Fund has reported on the limited understanding of ML/TF risks by Rosfinmonitoring and the Central Bank who neglect high-risk money laundering sectors outside the banking sector, such as real estate, legal services, and the trade of precious metals and stones (IMF 2016a).

Rosfinmonitoring also monitors how e-payment systems, such as QIWI and WebMoney, verify users' identity to prevent illicit transactions (Khrustaleva 2017). According to the Federal Law on ML/FT, an anonymous account balance must have a limit of 15,000 rubles (226 USD) and total operations with the account must not exceed 40,000 rubles a month (603 USD). For all other types of e-wallets, an e-payment system must verify the owner's identity.

FinCERT is a financial intelligence unit in the Central Bank of Russia. It analyses criminal incidents in the field and organises information exchange among financial institutions to detect fraudulent and suspicious operations. In 2017, there were 418 banks, mobile operations, telecom companies, energy companies, and IT-companies participating in the exchange (FinCERT Bank of Russia 2017). In 2018, the number rose to 718 organisations. Since July 2018, financial organisations are obliged to inform the Central Bank about all suspicious incidents (FinCERT Bank of Russia 2018).

One of the main AML/TF tools the regulator has involves revoking bank licences (Lavronenko 2018a). In 2017, 51 licences were revoked for violating banking legislation and the Central Bank regulations; 17 of the 51 licences were revoked for carrying out dubious transactions and 24 for non-compliance with Federal Law 115 on

AML/FT. The regulator estimated that over 300 billion rubles (4.5 billion USD) had been embezzled from the banks whose licenses were revoked (Rosfinmonitoring 2017).

In 2015, Russia signed 14 bilateral agreements with the members of the Egmont group to promote closer cooperation in investigating financial crimes (Rosfinmonitoring 2016). Russia's financial regulator also reported an increase in inquiries from foreign financial intelligence to battle international crimes. However, researchers suggest that more needs to be done regarding AML/FT regulations in the Eurasian region (Verevkin and Verevkin 2017).

Conclusion

To examine criminal ecosystems and transactional methods in cyberspace in Russia, we conducted a systematic review of the existing literature, industry reports, regulatory and research papers in the Russian language, as well as in English where it was relevant. The objective of the review was to summarise the state of knowledge on cyber offender business models, the criminal supply chain, the use of fiat and virtual currencies, and current law enforcement and industry practices within this area.

At the beginning of the project, we expected a lack of previous in-deep research on the subject in Russia, and this expectation was confirmed at the review stage. Few reports and papers described and assessed the transactions and transactional methods of cybercriminals after they obtain money. Therefore, to find trends, we also relied on separate cases of cybercriminal schemes reported by the press.

Leading information security companies such as Group-IB, BI.ZONE, and Positive Technologies had the most relevant and up-to-date reports with useful insights. They were also an important source of any numeric data regarding criminal proceeds, costs of operations, and losses to cybercrime in Russia. The Central Bank of Russia also published some of this data; however, their numbers were sometimes lower than the numbers reported by the industry experts. Most academic papers we consulted lacked original research on the money trail and often discussed general issues, such as proposed changes to legislation, typology of crimes and their evolutions, and foreign practices. However, some academic papers turned out to be a good source of anecdotal evidence.

Researching virtual currencies used by criminals in Russia was particularly challenging. While there is an abundance of papers on virtual currencies, most of them only cover principles of work, big international cases, absent legislation in Russia, and forecasts of how cryptocurrency can be used by criminals. Some studies mention virtual payment systems that are heavily used in Russia and illustrate that they can be daisy-chained in order to move relatively large volumes of money; however, the strategies offenders employ are often ignored by the investigators and not underpinned by any detailed reporting. Moreover, it is evident that Russian law enforcement has limited investigative capacity to pursue cybercrime. As a result, despite the volume of cybercrime that occurs within and emanates from Russia, the challenges that Russian law enforcement face echo the reported difficulties external investigators have researching all but the most egregious cybercrimes in Russia.

Works Cited

Ablon, Lillian, Martin C Libicki, and Andrea A Golay. 2014.*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Monica, CA: Rand Corporation.

Abrosimova, Nina. 2017. “Politsiya likvidirovala RAMP — krupneshiy v Rossii internet-magazin narkotikov.” [Police terminated RAMP, Russia’s biggest internet drug marketplace]. *Novaya gazeta*, 19 September 2017. https://www.novayagazeta.ru/articles/2017/09/19/73896-politsiya-likvidirovala-ramp-krupneshiy-v-rossii-internet-magazin-narkotikov

Alexandrov, I. S. 2018. "Nekotoryye Tendentsii Sudebnoy Praktiki Rassmotreniya Ugolovnykh Del O Prestupleniyakh, Predusmotrennykh St. St. 174, 174.1 Uk Rf, Sovershennykh S Ispol'zovaniyem Kriptovalyuty." [Some Trends of Judicial Practice Considering Criminal Cases on Crimes Envisaged by Articles 174, 174.1 of the Criminal Code of the Russian Federation Committed with Use of Cryptocurrency]. *Ugolovnoye pravo*, no. 6.

Alifanova E. N., and Yu. S. Evlakhova. 2016. "Uyazvimosti Finansovykh Institutov I Domokhozyaystv K Risku Otmyvaniya Deneg I Finansirovaniya Terrorizma: Analiz Vzaimosvyazey I Posledstviy V Kontekste Finansovoy Bezopasnosti." [Vulnerubilities of financial institutions and households in the face of money laundering and financing of terrorism: Analysing links and consequences of financial security]. *Finansovaya analitika: problemy i resheniya*, no. 18: 25-33.

Anapolskaya A. I., and M. Yu. Dvoretsky. 2019. "Osnovnyye Sposoby I Mekhanizm Legalizatsii (Otmyvaniya) Dokhodov, Poluchennykh Prestupnym Putem S Ispol'zovaniyem Elektronnykh Raschetnykh Operatsiy." [The main methods and mechanism of legalization (laundering) of criminally obtained income using electronic payment transactions]. *Vestnik instituta: Prestupleniye, nakazaniye, ispravleniye.*

Vologodskiy institut prava i ekonomiki federal'noy sluzhby ispolneniya nakazaniy (Vologda) 13, no. 1: 53-58.

Antonova E. Yu., and A. K. Klimenko. 2017. "Klassifikatsiya Khishcheniy Denezhnykh Sredstv S Ispol'zovaniyem Sredstv Svyazi." [A Classification of Embezzlements Using Means of Communication]. *Rossiyskiy sledovatel'*, no. 1 (2019): 38-41.

Arzamastsev, M. V. 2017. "K Voprosu Ob Ugolovno-Pravovoy Klassifikatsii Kiberprestupleniy." [On the topic of legal and criminal classification of cybercrime]. *Ugolovnoye pravo*, no. 1(3).

Bagmet, A. M. 2017. "Sledy-"Nevidimki"." [Invicible Traces]. *Sledstviyem ustanovleno*, no. 2 : 10-14.

Bank of Russia. 2019. "Obzor Nesanktsionirovannykh Perevodov Denezhnykh Sredstv Za 2018 God." [Overview of unsanctioned monetary transactions in 2018] FinCERT of Bank of Russia.

Bank of Russia. 2018. “Otchet tsentra monitoringa i reagirovaniya na komp'yuternyye ataki v kreditno- finansovoy sfere departamenta informatsionnoy bezopasnosti Banka Rossii 1.09.2017 – 31.08.2018.”[Report of the Centre for monitoring and reacting to computer attacks in the financial field from the chief department for security and protection of information of the Bank of Russia 1.09.2017 – 31.08.2018.]. Moscow: Central Bank of Russia.

Bank of Russia. 2017. “1 iyunya 2016 – 1 sentyabrya 2017. Otchet tsentra monitoringa i reagirovaniya na komp'yuternyye ataki v kreditno-finansovoy sfere glavnogo upravleniya bezopasnosti i zashchity informatsii Banka Rossii.” [1 June 2016 – 1 September 2017. Report of the Centre for monitoring and reacting to computer attacks in the financial field from the chief department for security and protection of information of the Bank of Russia]. Moscow: Central Bank of Russia.

Bankir.ru. 2016. "Pol Makkri (Visa): «Lyudi Ne Khotyat Platit', Oni Khotyat Pokupat'»." [Visa's Paul McCrea: People don't want to pay, they want to buy]. *Bankir.ru*, 15 August 2016. https://bankir.ru/publikacii/20160815/pol-makkri-visa-lyudi-ne-khotyat-platit-oni-khotyat-pokupat-10007916/

Batukhtin M. E., and S. S. Samchenko. 2018. "Kiberprestupleniya: Prichiny, Vidy, Formy, Posledstviya, Napravleniya Protivodeystviya." In *XX vserossiyskaya studencheskaya nauchno-prakticheskaya konferentsiya Nizhnevartovskogo* *gosudarstvennogo universiteta*, edited by A. V. Korichko, 24-27. Nizhnevartovsk: Nizhnevartovskiy gosudarstvennyy universitet.

Bayoumy, Yara. 2018. "Cybercrime Economy: A netnographic study on the Dark Net ecosystem for ransomware." NTNU.

Bazhanov S.V., and A.A Vorontsov. 2017. "Sposoby Vyvoda Za Rubezh Imushchestva I Denezhnykh Sredstv, Poluchennykh Nezakonnym Putem, a Takzhe Dokhodov Ot Takogo Imushchestva Kak Element Kriminalisticheskoy Kharakteristiki Sootvetstvuyushchikh Prestupleniy." [Means of Offshoring Illegally Received Property and Cash and Proceeds from Such Property asElement of Criminal Characteristics of Corresponding Crimes]. *Bezopasnost' biznesa*, no. 4.

Bazhanov, S. V. 2018. "Preduprezhdeniye V Kreditnykh Organizatsiyakh Khishcheniy Denezhnykh Sredstv S Ispol'zovaniyem Poddel'nykh Platezhnykh Kart, a Takzhe Putem Nezakonnogo Dostupa V Ikh Informatsionno-Telekommunikatsionnyye Seti." [Prevention of Embezzlements in Credit Institutions Involving Counterfeit Payment Cards and Illegal Access to the Information and Telecommunication Networks]. *Bezopasnost' biznesa*, no. 5.

BBC. 2019. “V Moskve proshel miting protiv izolyatsii runeta.” [Rally against internet isolation held in Moscow]. *bbc.com,* 10 March 2019 https://www.bbc.com/russian/news-47514303

Belokhrebtov, V. S. 2017. "Protivodeystviye Prestupleniyam, Svyazannym S Nezakonnym Obnalichivaniyem Denezhnykh Sredstv." [Countering crimes related to unlawful cash-out]. *Izvestiya tul'skogo gosudarstvennogo universiteta. Ekonomicheskiye i yuridicheskiye nauki*, no. 4-2: 82-87.

Belousov, D. M. 2015. "Aktual'nyye Voprosy Rassledovaniya Nezakonnogo Vyvoda Denezhnykh Sredstv Za Rubezh." [Pressing issues of investigation into illegal transfer of assets abroad]. *Zakonnost'*, no. 3.

Belousova, V. and Chichkanov, N. 2015. "Mobile Banking Adoption in Russia: What Incentives Matter?" In *Science, Technology, Innovation Economy*: Higher School of Economics.

Bespalov D.N., and M.A.Kazakov. 2014. "Informatsionnaya Voyna I Obespecheniye Bezopasnosti." [Information warfare, threats and information security]. *Vestnik MGIMO universiteta, Moskva*, no. 6 (39): 82-87.

BI.ZONE. 2019. “Threat Zone'19**:** False sense of cybersecurity.” *BI.ZONE Cybersecurity Sberbank*. Moscow.

Bondar E. O., and S. V. Izutina. 2018. "Naiboleye Rasprostranyonnyye Sposoby Legalizatsii (Otmyvaniya) Dokhodov, Poluchennykh Prestupnym Putem, I Finansirovaniyu Terrorizma." [The most common methods of legalization (laundering) of proceeds from crime and financing of terrorism]. *Aktual'nyye problemy administrativnogo prava i protsessa*, no. 1: 33-36.

Borogan I., and A. Soldatov. 2018. "Russia’s Approach to Cyber: The Best Defence Is a Good Offence." *Chaillot papers*, no. 148: 15-23.

Bottazzi, Giovanni, and Gianluigi Me. 2015. "A Survey on Financial Botnets Threat." International Conference on Global Security, Safety, and Sustainability.

Butenko, A.A. 2016. "Protivopravnaya Deyatel'nost' Po Obnalichivaniyu Beznalichnykh Denezhnykh Sredstv." [Illegal activity of cashing out digital funds]. *Obshchestvo i pravo*, no. 2(56): 72-75.

Chernenko, E. 2017. “Protivobotstvo sverkhderzhav.“ [Opposition between two empires]. *Kommersant*, 13 April 2017. https://www.kommersant.ru/doc/3270121

Chernyshova, Yevgenia. 2019 "V Rossii Zapretyat Anonimnoye Popolneniye Koshel'kov «Yandeks.Den'gi» I Qiwi." [Russia to ban anonymous top-up of Yandex.Money and QIWI e-wallets]. *RBC,* 29 July 2019. https://www.rbc.ru/finances/29/07/2019/5d3b00db9a7947f7ddbd3787

Chrepa, Eleni, Olga Kharif and Kartikay Mehrotra. 2018."Bitcoin Suspect Could Shed Light on Russian Mueller Targets." *Bloomberg*, , 4 September 2018. https://www.bloomberg.com/news/articles/2018-09-04/bitcoin-suspect-could-shed-light-on-russians-targeted-by-mueller

Coin ATM Radar. 2019. "Bitcoin ATMs in Russian Federation." Coin ATM Radar. https://coinatmradar.com/country/177/bitcoin-atm-russian-federation/.

Commonwealth of Independent States. 2016. “Resheniye ot 16 sentyabrya 2016 goda o Programme sotrudnichestva gosudarstv – uchastnikov Sodruzhestva Nezavisimykh Gosudarstv v bor'be s prestupleniyami, sovershayemymi s ispol'zovaniyem informatsionnykh tekhnologiy, na 2016–2020 gody.” [Decision on the Programme of the Commonwealth of States from 16 September 2016 regarding fighting crimes committed with information

technology covering 2016-2020]. ***CIS.*** http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=5476

Cyphort. 2015. *Cyphort Labs Knocks Down the Top 8 Financial Malware.* Santa Clara, CA: Cyphort, Inc.

Didikin, A.B. 2018. "Pravovoye Regulirovaniye Operatsiy S Kriptovalyutami: Problemy I Perspektivy." [Legal regulations of the operations with cryptocurrencies: problems and perspectives]. *Pravo i gosudarstvo* 3-4 (80-81): 121-30.

Digital Shadows Photon Research Team. 2019. *A Tale of Epic Extortions How Cybercriminals Monetize Our Online Exposure.* London: Digital Shadows. https://www.bbc.com/russian/news-47514303

Dolgieva, M. M. 2018. "Kvalifikatsiya Prestupleniy, Sovershayemykh V Sfere Komp'yuternoy Informatsii V Otnoshenii Kriptovalyuty." [Questions of Qualification of Crimes Committed in the Field of Computer Information in Relation to Cryptocurrencies]. *Sovremennoye pravo*, no. 11.

Dolgieva, M. M. 2018. "Sotsial'naya Obuslovlennost' Vozniknoveniya Ugolovno-Pravovykh Zapretov Narusheniy, Sovershayemykh V Sfere Oborota Kriptovalyuty." [Social prerequisits for the emergence of criminal law prohibitions of violations committed in the field of cryptocurrency turnover]. *Aktual'nyye problemy rossiyskogo prava*, no. 10.

Dolgieva, M. M. 2018. "Kriptoprestupnost' Kak Novyy Vid Prestupnosti: Ponyatiye, Spetsifika." [Cryptocrime as a New Type of Crime: Concept and Specificity]. *Sovremennoye pravo*, no. 10.

Dolgieva, M. M. 2018. "Kriptovalyutnaya Narkotorgovlya V Rossii I Za Rubezhom." [Cryptocurrency drug trafficking in Russia and abroad]. *Vestnik Voronezhskogo instituta MVD Rossii*, no. 4.

Dolgieva, M. M. 2018. "Konfiskatsiya Kriptovalyuty." [Confiscation of Cryptocurrency]. *Zakonnost'*, no. 11.

Dudin M. N., and N. V. Lyasnikov. 2018. "Ispol'zovaniye Kriptovalyuty V Nezakonnykh Tselyakh: Obespecheniye Finansovo-Ekonomicheskoy Bezopasnosti." [Using cryptocurrency illegally: establishing financial security]. *Problemy rynochnoy ekonomiki*, no. 3: 16-23.

Dulskaya, E. G. 2018. "Vozmozhnosti Ispol'zovaniya Spetsial'nykh Znaniy Pri Rassledovanii Prestupleniy, Svyazannykh S Nezakonnym "Obnalichivaniyem" Denezhnykh Sredstv." [Ways to use special knowledge when investigating crimes of illegal cashing-out]. *Deyatel'nost' pravookhranitel'nykh organov v sovremennykh usloviyakh. Sbornik materialov XXIII mezhdunarodnoy nauchno-prakticheskoy konferentsii*: 149-53.

Duma.gov.ru. 2018. “Zakonoproyekt № 419059-7 O tsifrovykh finansovykh aktivakh.” [Draft bill on digital financial assets № 419059-7]. Gosduma. https://sozd.duma.gov.ru/bill/419059-7

Eremina, Anna. 2016. "Sud Vzyskal 470 Mln Rubley S Protsessingovoy Kompanii Ucs." [Court exacted 470 mln from UCS processing company]. *Vedomosti*. 6 June 2016.https://www.vedomosti.ru/finance/articles/2016/06/07/643842-sud-vziskal-470-mln-rublei-protsessingovoi-kompanii-ucs

Eriashvili N.D., A.I. Grigor'yev and N.N. Nevskiy. 2018. "Bankovskoye Moshennichestvo: Skhemy Obmana Kliyentov Bankov I Nezakonnoye Obnalichivaniye Denezhnykh Sredstv." [Bank fraud: fraudulent schemes towars clients and illegal cash-out]. *Bulletin of Moscow Academy of the Investigative Committee of the RF*.

Europol. 2018. "The Internet Organised Crime Threat Assessment (IOCTA)." The Hague: Europol.

Europol. 2016. “**No more ransom: Law enforcement and its security companies join forces to fight ransomware” [Press release]. *Europol*.** https://www.europol.europa.eu/newsroom/news/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-to-fight-ransomware

Europol. 2015. "The Internet Organised Crime Threat Assessment (IOCTA)." The Hague: Europol.

FATF. 2014. "Annual Report 2013 - 2014 ": FATF.

FATF. 2013. "6th Follow-up Report Mutual Evaluation of the Russian Federation ": FATF.

Feoktistov, D. A. 2018. "Protivodeystviye Prestupnoy Deyatel'nosti, Sovershayemoy S Ispol'zovaniyem Kriptovalyut." [Combatting illicit activity using cryptocurrency]. In *Sovremennost' v tvorchestve nachinayushchego issledovatelya*. Irkutsk: Vostochno-Sibirskiy institut Ministerstva vnutrennikh del Rossiyskoy Federatsii.

Filimonov, S. A. 2014. "Nekotoryye Problemy Bor'by S Kiberprestupnost'yu Kak Samykh Opasnykh Transnatsional'nykh Prestupleniy." [Some problems of combating cybercrimes as most dangerous transnational crimes]. *«apriori. Ceriya: Gumanitarnyye nauki», www.Apriori-journal.Ru*, no. 1.

FinCERT Bank of Russia. 2018. "Otchet Tsentra Monitoringa I Reagirovaniya Na Komp'yuternyye Ataki V Kreditno-Finansovoy Sfere Departamenta Informatsionnoy Bezopasnosti Banka Rossii 1.09.2017 – 31.08.2018 ". Moscow: FinCERT Bank of Russia.

FinCERT. 2017. "Otchet Tsentra Monitoringa I Reagirovaniya Na Komp'yuternyye Ataki V Kreditno-Finansovoy Sfere Glavnogo Upravleniya Bezopasnosti I Zashchity Informatsii Banka Rossii." Moscow: FinCERT Bank of Russia.

Gadzhiev, S. N. 2018. "Tsifrovyye Valyuty Kak Ugroza V Sfere Pod/Ft." [Digital currencies as a threat in AML/FT]. *Sovremennyye nauchnyye issledovaniya i razrabotki. Izdatel'stvo: Nauchnyy tsentr "Olimp"*, no. 8(25) (2018): 55-57.

Gilinsky, Ya.I. "Problemy Sotsial'nogo Kontrolya Nad Prestupnost'yu V Sovremennom Obshchestve." [Problems of social control over criminality in the modern society]. *Kriminalist*, no. 4(25).

Gorokhova, S. S. 2018. "Kreditnyye Organizatsii V Sisteme Protivodeystviya Finansirovaniyu Terrorizma I Legalizatsii Dokhodov, Poluchennykh Prestupnym Putem." [Credit Institutions in the Anti-Money Laundering and Counter-Terrorism Financing System]. *Bankovskoye pravo*, no. 5.

Goryacheva, Veronika, and Vladislav Trifonov. 2019. "Sanatsiya Propustila «Otkrytiye»." [Bailout missed "Otrkrytiye"] *Kommersant*, 5 August 2019. https://www.kommersant.ru/doc/4052451

Goryacheva, Veronika. 2018. "Glavu Cobalt Arestovali." [Head of Cobalt arrested] *Kommersant*, 26 March 2018. https://www.kommersant.ru/doc/3585359

Goryashko, S. 2019. "Putin pobedil. Chto raskryl doklad Myullera o Trampe i o Kremle." [Putin has won. What Muller's report told about Trump and Kremlin]. *bbc.com*, 19 April 2019. https://www.bbc.com/russian/features-47982317

Greenberg, Andy. 2014. "An interview with Darkside, Russia's favorite dark web drug lord." *WIRED*, 12 April 2014. https://www.wired.com/2014/12/interview-darkside-russias-favorite-dark-web-drug-lord/

Group-IB 2019. “Silence 2.0. Going global”. Moscow: Group-IB.

Group-IB. 2018. "The Hi-Tech Crime Trends." Moscow: Group-IB.

Group-IB. 2018. “Group-IB: Cobalt’s latest attacks on banks confirms connection to Anunak”. *Group-IB*, 29 May 2018b. https://www.group-ib.com/media/group-ib-cobalts-latest-attacks-on-banks-confirms-connection-to-anunak/

Group-IB. 2014. "The Hi-Tech Crime Trends." Moscow: Group-IB, 2017.

Holt, Thomas J, and Olga Smirnova. "Examining the Structure, Organization, and Processes of the International Market for Stolen Data." Washington DC: *National Criminal Justice Reference Service.*

Holt, Thomas J, Olga Smirnova, and Yi-Ting Chua, eds. 2016. *Data Thieves in Action: Examining the International Market for Stolen Personal Information*. New York: Springer/

Holub, Artsiom, and Jeremiah O'Connor. 2018. "COINHOARDER: Tracking a Ukrainian Bitcoin phishing ring DNS style." 2018 APWG Symposium on Electronic Crime Research (eCrime).

Homeland Security. 2017. “Enhanced Analysis of GRIZZLY STEPPE Activity. Reference Number: AR-17-20045”. Washington: National Cybersecurity and Communications Integration Center.

IMF. 2016. "Russian Federation Financial Sector Assessment Program. Technical Note Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)." Washington: IMF.

IMF. 2016. "Russian Federation Financial Sector Assessment Program." Washington: IMF.

IMF. 2016. “Russian Federation Financial Sector Assessment Program. Technical note on anti-money laundering and combating the financing of terrorism (AML/CFT).” Washington: International Monetary Fund.

Itschenko, E. P. 2015. "O Kriminalisticheskom Obespechenii Raskrytiya I Rassledovaniya Kiberprestupleniy."[On criminological technics to investigate cybercrime]. In *Deyatel'nost' pravookhranitel'nykh organov v sovremennykh* *usloviyakh*, 336-41. Irkutsk: Vostochno-Sibirskiy institut Ministerstva vnutrennikh del Rossiyskoy Federatsii.

Izoldina, L. M. 2018. "Dokhody Ot Operatsiy S Kriptovalyutoy." [Proceeds of cryptocurrency operations]. *Nalog na pribyl': uchet dokhodov i raskhodov*, no. 12.

Izutina, S. V. 2018. "Problemy Bor'by S Legalizatsiyey Prestupnykh Dokhodov: Opyt I Perspektivy." [Problems of Combating the Criminal Proceeds' Legalization: Experience and Prospects]. *Ekonomika. Pravo. Obshchestvo. Rossiyskiy ekonomicheskiy universitet imeni G.V. Plekhanova (Moskva)*, no. 4(16).

Kalashnikova E. B., and M. A. Arkhipov. 2018. "Osnovnyye Mekhanizmy, Ispol'zuyemyye Pri Otmyvanii Prestupnykh Dokhodov, Poluchennykh Ot Kiberdeyatel'nosti." [Common schemes used in laundering proceeds of cyberactivity]. *«Nauchno-prakticheskiy elektronnyy zhurnal Alleya Nauki»*, no. 11 (27).

Kamaletdinov, Damir. 2019. "V Rossii Novyy Bum Bankovskogo Moshennichestva Po Telefonu. Kak Ne Popast'sya I V Chyom Mogut Byt' Prichiny." [There's a new banking fraud via phone boom in Russia. How not to become a victim and why it may be happening] *TJournal*, 12 August 2019. https://tjournal.ru/analysis/110591-v-rossii-novyy-bum-bankovskogo-moshennichestva-po-telefonu-kak-ne-popastsya-i-v-chem-mogut-byt-prichiny.

Kardakov V. A., and Z. M. Gizatullin. 2018. "Fishing S Ispol'zovaniyem Mashinnogo Obucheniya." In *Natsional'naya bezopasnost' Rossii: Aktual'nyye aspekty*, 13-17. St. Petersburg: Gumanitarnyy natsional'nyy issledovatel'skiy institut «NATSRAZVITIYE».

Kaspersky. 2019. "Financial Cyberthreats in 2018." Kaspersky Lab.

Kaznova M. I., and A. E. Ovchinnikova. 2017. "Ispol'zovaniye Elektronnykh Sredstv Platezha V Tselyakh Otmyvaniya Denezhnykh Sredstv I Finansirovaniya Terrorizma." In *Vyzovy i vozmozhnosti finansovogo obespecheniya stabil'nogo ekonomicheskogo rosta (finansy-2017)*, edited by «Sevastopol'skiy gosudarstvennyy universitet», 21-26. Sevastopol: Ribest.

Khaidarshina, R. F. 2018. "Obzor Kiberprestupleniy, Sovershennykh V 2017." [Overview of cybercrimes commited in 2017]. *«Nauchno-prakticheskiy elektronnyy zhurnal Alleya Nauki»*, no. 4(20).

Khaliullin, A. 2014. “Podkhody k opredeleniyu prestupleniy v informatsionno-telekommunikatsionnykh setyakh.” [Approached to defining crime in information-telecommunications networks]. *Pravo i Kiberbezopasnost'*, 2, 19-26.

Khaliullina, E.T. 2018. "Lichnost' Komp'yuternogo Prestupnika V Sovremennoy Rossii." [Computer criminal profile in the modern Russia]. *Bulletin of Moscow Academy of the Investigative Committee of the Russian Federation*, no. 2: 90-97.

Khisamova, Z. I. 2017. "Sposoby Legalizatsii (Otmyvaniya) Dokhodov, Poluchennykh Prestupnym Putem, S Ispol'zovaniyem Informatsionno-Telekommunikatsionnykh Tekhnologiy." [Methods of legalization (laundering) of incomes from crime through the use of information and telecommunication technologies]. *Vestnik Krasnodarskogo Universiteta MVD Rossii* 2(36): 84-87.

Khrustaleva, A. V. 2017. "Isklyucheniye Riska Legalizatsii (Otmyvaniya) Dokhodov, Poluchennykh Prestupnym Putem, I Finansirovaniya Terrorizma Operatorom Po Perevodu Elektronnykh Denezhnykh Sredstv." [Limiting risks of laundering of proceeds of crime and the financing of terrorism by an e-money transfer operator]. *Bankovskoye pravo*, no. 1.

Kirillova, A. S. 2018. "Kiberprestupnost' V Rossiyskoy Federatsii: Osnovnyye Problemy I Sposoby Ikh Resheniya." In *Yevraziyskaya yuridicheskaya konferentsiya*: MTSNS «Nauka i prosveshcheniye».

Komarov, A. 2016. “O tselesoobraznosti ispol'zovaniya “kiberterminologii” v issledovanii problem prestupnosti.” [On expediency of using cyberterminology in researching problems of crime]. *Informatsionnoye parvo*, 1, 4-7.

Kondrashin, M. 2018. ""Chernyye Lebedi" Informatsionnoy Bezopasnosti." [Black swans of information security]. *Bankovskoye obozrenie*, no. 10.

Kondrat, E. N. 2016. "Kreditnyye Organizatsii I Prestupnyye Skhemy "Obnalichivaniya" Denezhnykh Sredstv I Vyvoda Za Rubezh." [Credit and criminal schemes of cashing money and export abroad]. *Yuridicheskaya nauka: Istoriya i sovremennost'*, no. 9 : 114-24.

Korchagin, O.N. 2016."Tipologii Legalizatsii (Otmyvaniya) Dokhodov Ot Nezakonnogo Oborota Narkotikov." [Types of proceeds laundering from drug trafficking]. *Rossiyskiy sledovatel'*, no. 20.

Koshkina, Yulia. 2017. “Kliyent vsegda neprav?” [Is the client always wrong?] *Banki.ru*. https://www.banki.ru/news/daytheme/?id=10904685

Kraemer-Mbula, Erika, Puay Tang, and Howard Rush. 2013. "The cybercrime ecosystem: Online innovation in the shadows?" *Technological Forecasting Social Change* 80 (3): 541-555.

Kravtsov, D. A. 2018. "Nekotoryye Aspekty Preduprezhdeniya Kiberprestupnosti." [A few aspects of preventing cybercrime]. *Rassledovaniye prestupleniy: problemy i puti ikh resheniya*, no. 4: 57-60.

Kremlin.ru. 2020. “Strategiya natsional'noy bezopasnosti Rossiyskoy Federatsii do 2020 goda.” [National Security Doctrine of the Russian Federation until 2020]. Moscow: Kremlin, 2009. http://kremlin.ru/supplement/424

Krivorotova, Anastasiya, Lyudmila Petukhova, Anna Mikheyeva, Natal'ya Novopashina and Aleksey Pastushin. 2018. "Tsb Otsenil Tenevoy Oborot Moskovskikh Rynkov V 600 Mlrd Rub." [Central Bank estimates grey Moscow market activities at 600 billion rubles] *RBC*, 12 April 2018. https://www.rbc.ru/finances/12/04/2018/5acf26f59a79471ae61bfbc9

Kujawa, Adam, Wendy Zamora, Jovi Umawing, Jerome Segura, William Tsing, Adam McNeil, Pieter Arntz, and Chris Boyd. 2018. Cybercrime tactics and techniques: Q3 2018. Malwarebytes Labs.

Kumachev, Aleksey, and Karashash Nogayeva. 2018. “Dark Nation. Kak izmenilas' ekonomika Chernoy seti spustya god posle zakrytiya RAMP.” [Dark Nation. How the darknet economics changed one year after RAMP shut down]. *dp.ru*. https://www.dp.ru/a/2018/07/11/Dark_Nation__Kak_izmenila

Kumukov, M. Sh. 2018. "Tekhnologiya Blokcheyn: Novyye Vyzovy I Vozmozhnosti V Sisteme Mer Po Pod/Ft (Protivodeystviye Otmyvaniyu Deneg I/Ili Finansirovaniyu Terrorizma)." [Blockchain: new challenges and opportunities in the system of AML/FT measures (anti-money laundering and/or countering the financing of terrorism)]. *Leningradskiy yuridicheskiy zhurnal*, no. 2.

Kupriyanov E. I., and S. V. Krasheninnikov. 2018. "Osobennosti Proizvodstva Otdel'nykh Sledstvennykh Deystviy Pri Rassledovanii Prestupleniy, Svyazannykh S Khishcheniyem Denezhnykh Sredstv So Schetov Bankovskikh Kart Posredstvom Ispol'zovaniya Elektronnykh Platezhnykh Sistem." [Peculiarities of Performance of Specific Investigatory Activities When Investigating Crimes Involving Embezzlement of Money from Bank Card Accounts Using Electronic Payment Systems]. *Rossiyskiy sledovatel'*, no. 6.

Kurbatov, A. Ya. 2019. "Nepersonifitsirovannyye Elektronnyye Sredstva Platezha: Poryadok I Problemy Ispol'zovaniya." [Anonymous Electronic Payment Facilities: The Procedure and Problems of Use]. *Bankovskoye pravo*, no. 2.

Lavronenko, R. A. 2018. "Aktual'nyye Problemy Protivodeystviya Legalizatsii Prestupnykh Dokhodov V Bankovskoy Sfere." [Relevant Issues of Anti-Money Laundering in the Banking Sector]. *Bezopasnost' biznesa*, no. 2.

Lavronenko, R. A. 2018. "Problemy V Deyatel'nosti Pravookhranitel'nykh Organov Pri Vyyavlenii, Raskrytii I Rassledovanii Legalizatsii Prestupnykh Dokhodov V Kreditno-Finansovoy Sisteme." [Issues in the Activities of Law Enforcement Bodies in Identification, Detection and Investigation of Money Laundering in the Credit and Finance System]. *Rossiyskiy sledovatel'*, no. 3.

Lavronenko, R. A. 2018. "Legalizatsiya Prestupnykh Dokhodov, Sovershayemaya V Kreditno-Finansovoy Sisteme S Ispol'zovaniyem Kriptovalyuty." [Money Laundering in the Credit and Finance System Involving Cryptocurrency Use]. *Bezopasnost' biznesa*, no. 5.

Lavronenko, R. A. 2018. "Problemy Mezhdunarodnogo Sotrudnichestva V Sfere Bor'by S Legalizatsiyey Prestupnykh Dokhodov V Kreditno-Finansovoy Sisteme." [Issues of International Cooperation in the Anti-money Laundering Sector in the Credit and Financial System]. *Mezhdunarodnoye ugolovnoye pravo i mezhdunarodnaya yustitsiya*, no. 2.

Lebedeva, A. A. 2018. "Aktual'nyye Voprosy Kvalifikatsii Moshennichestva V Sfere Komp'yuternoy Informatsii." [Relevant Issues of Cyber Fraud Qualification]. *Bezopasnost' biznesa*, no. 5.

Lebedeva, A. A. 2018. "Khishcheniye Denezhnykh Sredstv So Schetov Platezhnykh Kart." [Embezzlement from Bank Card Accounts]. *Bezopasnost' biznesa*, no. 1.

Levchenko, Lyova. 2017. “Chto sluchilos' s krupneyshim rossiyskim narkorynkom v darknete.» [What happened to Russia’s biggest drug marketplace on darknet]. *The Village*. https://www.the-village.ru/village/weekend/weekend-comments/283928-ramp

Likholetov, A. A. 2017. "Problemy Razgranicheniya Moshennichestva S Ispol'zovaniyem Platezhnykh Kart S Drugimi Sostavami Prestupleniy." [Problems of delineation of fraud using payment cards from other offences]. *Rossiyskaya yustitsiya*, no. 6.

Linnikov, A.S. 2017. "Ekonomicheskiye Posledstviya Rasshireniya Masshtabov Kiberprestupnosti V Rossii I Mire." [Economic consequences of cybercrime expansion in Russia and the world]. *Bankovskoye pravo*, no. 5.

Loshkarev, V. V. 2016. "Protivodeystviye Nezakonnomu Obnalichivaniyu Denezhnykh Sredstv." [Fight against unlawful cashing out of funds]. *Zakonnost'*, no. 11.

Makarov A. V., and V. A. Aleshkova. 2019. "Osobennosti I Problemy Kvalifikatsii Moshennichestva, Sovershennogo S Ispol'zovaniyem Elektronnykh Sredstv Platezha." [Peculiarities and Issues of Classification of Fraud Committed Using Electronic Payment Means]. *Rossiyskiy sud'ya*, no. 5.

Mandiant. M-Trends. 2017. *A View from the Front Lines*. FireEye.

Markaryan, E. S. 2018. "Spetsifika Provedeniya Sledstvennogo Osmotra Pri Rassledovanii Prestupleniy, Sovershennykh S Ispol'zovaniyem Kriptovalyut." [Specifics of investigatory examination in the investigation of crimes committed involving cryptocurrency]. *Aktual'nyye problemy rossiyskogo prava*, no. 6.

Mediascope. 2019. “Elektronnyye platezhi rossiyan 2019 god.” [Electronic payments of Russian citizens in 2019]. *Mediascope*, 20 August 2019. https://money.yandex.ru/page?id=529500

Mihailova, N. S. 2019. "Рынок "Обнала" В Условиях Тотального Контроля." [The cash-out market in the conditions of total control]. *Ekonomika ustoychivogo razvitiya*, no. 1(37): 48-52.

Mikhaylov, Alexander, and Richard Frank. 2016. "Cards, money and two hacking forums: An analysis of online money laundering schemes." 2016 European Intelligence and Security Informatics Conference (EISIC).

Ministry of Foreign Affairs of Russia. 2018. “Press release on the adoption of a Russian resolution on international information security at the UN General Assembly.” Ministry of Foreign Affairs of Russia. http://www.mid.ru/en_GB/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3437775

Ministry of Interior. 2017. “MVD Rossii stalo ofitsial'nym partnerom mezhdunarodnogo proyekta po bor'be s kiberprestupnost'yu «Bol'she nikakikh vykupov!» - «No more ransom!».” [Russian Ministry of Interior is a partner in the international project for fighting cybercrime “No more ransom!”]. Ministry of Interior. https://xn--b1aew.xn--

p1ai/mvd/structure1/Upravlenija/Nacionalnoe_centralnoe_bjuro_Interpola/Publikacii_i_vistuplenija/item/9813461/

Mosechkin, I. N. 2015. "Problema Opredeleniya Neposredstvennogo Ob"Yekta Nezakonnykh Organizatsii I Provedeniya Azartnykh Igr." [Problem of determining the direct object of illegal organization and conduct of gambling activities]. *Российский следователь*, no. 14.

Nemova, M. I. 2018. "Ugolovno-Relevantnyye Riski Oborota Al'ternativnykh Sredstv Rascheta." [Relevant legal risks of distribution of alternative payment systems]. *Rossiyskiy sledovatel'*, no. 10.

Nikulina, O. A. 2015. "Sposoby Moshennichestva S Ispol'zovaniyem Platezhnykh Kart Kak Element Kriminalisticheskoy Kharakteristiki Dannogo Vida Prestupleniy." [Fraudulent methods in the use of bank cards as a criminal trait of this type of crime]. *Vestnik Voronezhskogo instituta FSIN Rossii* 4: 100-04.

Olinder, N. V. 2015. "Kriminalisticheskaya Kharakteristika Elektronnykh Platezhnykh Sredstv I Sistem." [Forensic characterization of Electronic Payment Means and Systems]. *Lex russica*, no. 10 .

Orlova I. A., V. V. Ilinova, and R. A. Ilinov. 2018. "Novyye Tekhnologii Platezhey I Raschetov Kak Sposob Otmyvaniya Deneg." [New payment and settlement technologies as a way of «money laundering»]. *Innovatsionnyye tekhnologii v mashinostroyenii, obrazovanii i ekonomike* 14, no. 1-2(7): 414-19.

Persianinov, Roman. 2017. “Ya nikogo ne trogayu, i oni menya ne trogayut: kak Telegram stanovitsya ploshchadkoy narkobiznesa.” [“I don’t bother anyone, and they don’t bother me”: How Telegram is becoming a drug dealer platform]. *TJournal*. https://tjournal.ru/tech/60100-drugsintelegram

Positive Technologies. 2018. "Kiberbezopasnost' — 2018−2019: Itogi I Prognozy." [Cybersecurity 2018-2019. Results and Forecasts]. Moscow: Positive Technologies.

Positive Technologies. 2018 "Rynok Prestupnykh Kiberuslug 2018." [Darknet cybermarkets 2018]. Moscow: Positive Technologies.

Positive Technologies. 2018. "Aktual'nyye Kiberugrozy - 2018. Trendy I Prognozy." [Relevant Cyberthreats 2018]. Moscow: Positive Technologies.

Positive Technologies. 2018. "Issledovaniye Zashchishchennosti Prilozheniy Dlya Treydinga." [Researching security of trading apps]. Moscow: Positive Technologies.

Positive Technologies. 2019. "Uyazvimosti Onlayn-Bankov 2019." [Online banks vulnerabilities]. Moscow: Positive Technologies.

Povetkina N.A., and Yu.V. Ledneva. 2018. ""Fintekh" I "Regtekh": Granitsy Pravovogo Regulirovaniya." [Fintech and Regtech: The Boundaries of Legal Regulation]. *Pravo. Zhurnal Vysshey Shkoly Ekonomiki*, no. 2.

Pravo.gov.ru. 2019. “Federal'nyy zakon ot 01.05.2019 № 90-FZ "O vnesenii izmeneniy v Federal'nyy zakon "O svyazi" i Federal'nyy zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii.” [Federal Law of 01.05.2019 № 90-FZ on amendments to the Federal Law on Communication and Federal Law on Information, information technology, and information protection]. Pravo.gov.ru. http://publication.pravo.gov.ru/Document/View/0001201905010025

Pravo.gov.ru. 2016. “Ukaz Prezidenta Rossiyskoy Federatsii ot 05.12.2016 № 646 "Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii.” [Russian President Decree of 05.12.2016 № 646 On Passing the Information Security Doctrine of the Russian Federation]. Pravo.gov.ru. http://publication.pravo.gov.ru/Document/View/0001201612060002

PwC. 2018. "Combating Fraud: Measures Taken by Companies. Russian Economic Crime and Fraud Survey 2018." PwC.

Revenkov P.V., and A.B. Dudka. 2015. "Riski Otmyvaniya Deneg V Usloviyakh Primeneniya Elektronnykh Dene." [Electronic money: Risks of money laundering]. *Vestnik Omskogo universiteta. Seriya «Ekonomika»*, no. 4: 78-88.

RIA Novosti. 2018. "V Shesti Gorodakh Rossii Po Trebovaniyu Tsb Iz"Yali Kriptomaty." [Russian ATMs seized in 6 cities at Central Bank request] *RIA Novosti*. https://ria.ru/20180903/1527738289.html

RIA Novosti. 2018. “V MVD soobshchili o kolichestve zaregistrirovannykh kiberprestupleniy v Rossii.” [Ministry of Interior reports on a number of registerd cybercrimes in Russia]. *RIA Novosti*. https://ria.ru/20180706/1524114695.html

RIA Novosti. 2017 “Kiberprestupnost' v Rossii vyrosla v shest' raz s 2013 goda.” [Cybercriminality in Russia had sixfold increase since 2013]. *RIA Novosti*, 29 November 2017a. https://ria.ru/20171129/1509843675.html

RIA Novosti. “V SPCH vystupili za prisoyedineniye Rossii k konventsii po kiberprestupnosti.” [Court for Human Rights advocated for Russia joining the cybercrime convention] *RIA Novosti,* 27 October 2017b. https://ria.ru/20171027/1507693950.html

RIA Novosti. 2016 "Tns: V Rossii 92% Internet-Pol'zovateley Pol'zuyutsya Online-Platezhami." [TNS: 92% of internet users on Russia use online-payments] *RIA Novosti*, 17 May 2016. https://ria.ru/20160517/1434854604.html

Rodina, E. 2017. "Dva Bicha Pod/Ft." [Two enemies of AML/FT]. *Bankovskoye obozrenie*, no. 8.

Rogozin, V.Y. 2015. "Novyye Realii Prestupnosti V Sfere Komp'yuternoy Informatsii." [New realities of the computer information criminality]. *Bulletin of Academy of the Investigative Committee of the Russian Federation*, no. 1: 138-141.

Rosfinmonitoring. 2017. "Rosfinmonitoring Activity Report." Rosfinmonitoring.

Rosfinmonitoring. 2016. "Publichnyy Otchet O Deyatel'nosti Federal'noy Sluzhby Po Finansovomu Monitoringu 2015." Moscow: Rosfinmonitoring.

Rosfinmonitoring. 2014. “Informatsionnoye soobshcheniye «Ob ispol'zovanii kriptovalyut».” [Statement on cruptocurrency use]. Rosfinmonitoring. http://www.fedsfm.ru/news/957

Rostelecom. 2019 "Otchet O Ddos-Atakakh Na Rossiyskiye Kompanii V 2018 Godu." [Report on DDoS attacks on Russian companies in 2018]. Moscow: Rostelecom.

Rostelecom. 2018. "Godovoi Otchet 2018." [Yearly report 2018]. Moscow: Rostelecom.

Rostelecom. 2017. "Godovoi Otchet 2017." [Yearly report 2017]. Moscow: Rostelecom.

Rudakova Yu. S., and E. S. Dmitrieva. 2018."K Voprosu O Sposobakh Sovershenіya Khishcheniy Denezhnykh Sredstv Iz Bankomatov." In *Vserossiyskaya nauchno-prakticheskaya konferentsiya «Ugolovno-protsessual'nyye i kriminalisticheskiye problemy bor'by s prestupnost'yu»*, edited by Chaplygina V.N. Bulyzhkin A.V., Vasyukov V.F., Sretentsev A.N., 170-75. Orel: Orlovskiy yuridicheskiy institut MVD Rossiyskoy Federatsii imeni V.V. Luk'yanova.

Ruslyakova, N. A. 2018. "Obnalichivaniye Deneg Kak Odin Iz Sposobov Ukhoda Ot Nalogov." [Cashing out at a means of tax evasion]. *Nalogi*.

Russkevich, E. A. 2018. "Mezhdunarodno-Pravovyye Podkhody Protivodeystviya Prestupleniyam, Sovershayemym S Ispol'zovaniyem Informatsionno-Kommunikatsionnykh Tekhnologiy." [International law approaches to combating crimes committed using information and communication technology]. *Mezhdunarodnoye ugolovnoye pravo i mezhdunarodnaya yustitsiya*, no. 3.

SecureWorks. 2016.*Underground Hacker Markets; Annual Report—April 2016.* Dell.

Sedlov, Danil. 2016."Kontaktnyye Platezhi: Kak Rabotayet Servis Po Perevodu Deneg «Vkontakte»." [Contact payment: how VK payments work]. *RBK*, 21 September 2016. https://www.rbc.ru/money/21/09/2016/57e23ca79a79475109565a3d

Shaikhattarova, S. V. 2016. "Rossiya I Mezhdunarodnyye Standarty Po Bor'be S Kiberprestupnost'yu." [Russia and international standards of fighting cybercrime]. *Mezhdunarodnoye ugolovnoye pravo i mezhdunarodnaya yustitsiya*, no. 4 (2016).

Sharova, I. I. 2017. "Khishcheniye Elektronnykh Denezhnykh Sredstv." [Theft of electronic funds]. *Ugolovnoye pravo*, no. 1.

Shestoperov, Dmitriy and Danila Moiseyev. 2019. "Fsb Poluchit Razdelegiruyushchiye Polnomochiya." [FSB to get blocking rights] *Kommersant*, 6 August 2019. https://www.kommersant.ru/doc/4053073

Shevchenko, E. 2014. “O kriminalisticheskoy traktovke ponyatiya «kiberprestupnost».” [On criminological explanation of the cybercrime term]. *Pravo i Kiberbezopasnost’*, 2: 9-14.

Shokhin, S. O. 2018. "Problemy Pravovogo Obespecheniya Bor'by S Legalizatsiyey Nezakonno Poluchennykh Dokhodov V Yevraziyskom Ekonomicheskom Soyuze." [Issues of Legal Support of Anti-Money Laundering in the Eurasian Economic Union]. *Yurist*, no. 1.

Shubin, Mikhail. 2018. “On magnets or underground: how does the Russian anonymous marketplace work?” *Political Critique*, 24 October 2018. http://politicalcritique.org/cee/2018/on-magnets-or-underground-how-does-the-russian-anonymous-marketplace-work/

Sidorenko, E. L. 2018. "Kriptovalyuta Kak Predmet Khishcheniya: Problemy Kvalifikatsii." [Cryptocurrency as a Subject of Embezzlement: Qualification Issues]. *Mirovoy sud'ya*, no. 6.

Sidorenko, E. L. 2017. "Kriminologicheskiye Riski Oborota Kriptovalyuty." [Criminological Risks of Crypto Currency Turnover]. *Ekonomika. Nalogi. Pravo*, no. 6: 147-54.

Sidorenko, E. L. 2016. "Kriminal'noye Ispol'zovaniye Kriptovalyuty: Mezhdunarodnyye Otsenki." [Criminal Use of Cryptocurrency: International Assessments]. *Mezhdunarodnoye ugolovnoye pravo i mezhdunarodnaya yustitsiya*, no. 6.

Skovoroda A.A., and D.Y Gamayunov. 2017. "Analiz Mobil'nykh Prilozheniy S Ispol'zovaniyem Modeley Privilegiy I Api-Vyzovov Vredonosnykh Prilozheniy." [Analysing mobile apps using privilege model and API-calls of malware apps]. *Prikladnaya diskretnaya matematika*, no. 36: 84-105. https://doi.org/10.17223/20710410/36/7.

Smirnova, Olga, and Thomas Holt. 2017. "Examining the Geographic Distribution of Victim Nations in Stolen Data Markets." *American Behavioral Scientist* 61, no. 11: 1403-26.

Solar JSOC. 2018. "Analitiki Solar JSOC zafiksirovali pochti dvukratnyy rost chisla kiberatak v 2018 godu." [Solar JSOC analytics registered almost a twofold increase in cyber-attacks in 2018]. Solar JSOC, 2019. https://rt-solar.ru/products/jsoc/news_and_publishing/1604/

Solar JSOC. 2018. "Solar JSOC Security Flash Report. Pervoye polugodiye 2018 goda." Moscow.

Solar JSOC. 2017. "Solar JSOC Security Flash Report Pervoye Polugodiye 2017 Goda." Moscow.

Solar JSOC. 2017. "JSOC Security Flash Report Vtoroye Polugodiye 2017 Goda.".

Solar Security. "Issledovaniye Zashchishchennosti Mobil'nykh Koshel'kov Dlya Kriptovalyut." [Researching security of mobile crypto wallets]. Solar Security.

Sologub, Nikita. "MVD vs. RAMP: vret li narkopolitsiya o samoy uspeshnoy operatsii v svoyey istorii." [Ministry of Interior vs RAMP: Is the drug police lying about its most successful operation in history?] Mediazona, 22 September 2017. https://zona.media/article/2017/09/22/ramp

Soudijn, Melvin RJ, and Birgit CHT Zegers. 2012. "Cybercrime and virtual offender convergence settings." *Trends in Organized Crime* 15 (2-3): 111-129.

Stoyanov, Ruslan. 2013.*Russian Financial Cybercrime: How it works.* Kaspersky Lab, 2015.

Sukharenko, A. Global'nyy vyzov chelovechestvu. *Sodruzhestvo*, 4: 14-17.

Sukharenko, A. N. 2018."Konfiskatsiya Prestupnykh Dokhodov Po Prigovoram Inostrannykh Sudov." [Confiscation of Proceeds from Crime under Sentences of Foreign Courts]. *Mezhdunarodnoye publichnoye i chastnoye pravo*, no. 3: 28-30.

Symantec. 2018.“Subverting Democracy: How Cyber Attackers Try to Hack the Vote.” *Symantec*, 18 September 2018a. https://www.symantec.com/blogs/election-security/election-hacking-faq

Symantec. 2018. "Internet Security Threat Report." Symantec, 2018b.

Symantec 2019. "Internet Security Threat Report." Symantec, 2019.

TASS. 2017. “Rossiyskiy diplomat nazval Budapeshtskuyu konventsiyu po kiberprestupleniyam ustarevshey”. [Russian diplomate calls Budapest Convention on Cybercrime outdated]. *Tass.ru*, 4 December 2017. https://tass.ru/politika/4782506

Tatulnik, A. Ya. 2018. "K Voprosu O Bor'be S Nezakonnym Obnalichivaniyem Denezhnykh Sredstv." [On combating illegal cashing out]. *Sovremennost' v tvorchestve nachinayushchego issledovatelya. Sbornik materialov nauchno-prakticheskoy konferentsii molodykh uchenykh. Vostochno-Sibirskiy institut Ministerstva vnutrennikh del Rossiyskoy Federatsii* : 77-80.

The Shanghai Cooperation Organisation. 2018. “**SCO calls for safe functioning and development of internet.” SCO.** http://eng.sectsco.org/news/20180126/377347.html

Timofeev, A.V. 2016. "Vyyavleniye I Raskrytiye Kiberprestupleniy V Kreditno-Finansovoy Sfere." [The identification and detection of cybercrimes in credit-financial sphere]. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii* 3 (71): 137-40.

Truntsevsky Y. V., and A. N., and Sukharenko. 2018. "Protivodeystviye Ispol'zovaniyu Kriptovalyuty V Nezakonnykh Tselyakh: Sostoyaniye I Perspektivy." [Combating Illegal Use of Cryptocurrency: The Status and Prospects]. *Mezhdunarodnoye publichnoye i chastnoye pravo*, no. 1 (2019).

Truntsevsky, Y.V. 2016. "Sostoyaniye I Tendentsii Prestupnosti V Rossiyskoy Federatsii I Prognozy Yeye Razvitiya." [Status and trends of crime in the Russian Federation and forecast of its development]. *Rossiyskaya yustitsiya*, no. 8.

Truntsevsky, Y.V. 2018. "Tsifrovaya (Virtual'naya) Valyuta I Protivodeystviye Otmyvaniyu Deneg: Pravovoye Regulirovaniye." [Digital (virtual) currency and combating money laundering: legal regulations]. *Bankovskoye pravo*, no. 2.

Vasyukov V. F., A. V. Bulyzhkin. 2017. "Nekotoryye Osobennosti Rassledovaniya Prestupleniy, Sovershayemykh S Ispol'zovaniyem Elektronnykh Platezhnykh Yedinits." [Some Peculiarities of Investigation of Crimes Committed Using Electronic Payment Units]. *Rossiyskiy sledovatel'*, no. 23.

Veprev S.B., and S.A. Nesterovitch. 2018. "Kiberprestupnost' Kak Novaya Forma Prestupnosti." [Cybercrime as a new type of criminality]. *Rassledovaniye prestupleniy: problemy i puti ikh resheniya*, no. 3: 78-82.

Verevkin L. P., and A. A. Verevkin. 2017. "Kiberprestupnost' V Finansovoy Sfer." [Cybercrime in the financial sector]. *Energiya: ekonomika, tekhnika, ekologiya*, no. 1: 56-62.

VK. 2019. "What Are Votes and How Can You Buy Them?" VK, n/d, accessed 22 August, 2019, https://vk.com/faq10379?q=how%20to%20buy.

Voevodin A. Y., and A. S. Khatyreva. 2017. "Internet Veshchey: Innovatsionnaya Opasnost' Finansovogo Sektora Ekonomiki Rf." [The internet of things: Innovative Hazard of the financial sector of the economy of the Russian Federation]. *Nauchnyye zapiski molodykh issledovateley* 2: 58-62.

Yakovlev, A. B. 2019. "Protivodeystviye Legalizatsii (Otmyvaniyu) Dokhodov, Poluchennykh Prestupnym Putem, I Finansirovaniyu Terrorizma Kak Vid Finansovogo Kontrolya." [Counteraction to Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism as a Form of Financial Control]. *Aktual'nyye problemy rossiyskogo prava*, no. 5.

Yani, P.S. "Moshennichestvo S Ispol'zovaniyem Elektronnykh Sredstv Platezha." [Online payment fraud]. *Zakonnost'*, no. 4,5,6 (2019).

Zaernuyk V. M., and L. I. Chernikova. 2017. "Kiberriski — Global'naya Problema Sovremennosti (Na Primere Predpriyatiy Gornodobyvayushchey Otrasli)." [Cyber-risks — global problem of the present (the example of the enterprises of the mining industry)]. *Finansovaya zhizn'*, no. 4: 4-8.

Zakharov, A. 2019. “**Russian data theft: Shady world where all is for sale.”** *bbc.com***. 27 May, 2019. https://www.bbc.com/news/world-europe-48348307.**

Zakharov, Andrey, and Sergey Kozlovskiy.2019. "V Italii Zaderzhan Eks-Vladelets Kriptovalyutnoy Birzhi Wex Dmitriy Vasil'yev." [Ex-owner of the WEX cryptomarket Dmitriy Vasiliev detained in Italy]. *BBC News*, 19 July 2019. https://www.bbc.com/russian/news-49030535

Zhuravlevko N. I., and L. E. Shvedova. 2015. "Problemy Bor'by S Kiberprestupnost'yu I Perspektivnyye Napravleniya Mezhdunarodnogo Sotrudnichestva V Etoy Sfere." [Problems of combating cybercrime and future directions of international cooperation in this field]. *Obshchestvo i pravo*, no. 3(53): 66-70.

Section III: Lessons from the Sinophone Literature

Introduction

According to World Internet Statistics (Miniwatts Marketing Group, 2019), the global number of internet users in 2019 surpassed 4.5 billion. About a fifth of them (around 876 million) are located in Chinese speaking countries, including the People’s Republic of China (China) and Taiwan. With more than 854 million internet users, China has the most internet users in Asia and the world. China has an internet penetration rate of around 61.2% in 2019, with 98% of users accessing the internet primarily on a mobile phone (McCarthy 2018, CNNIC 2019). China still has room for a significant increase in internet users and mobile phones become more accessible to a greater proportion of the population. Taiwan has more than 22 million internet users, representing over 92 percent of its population. Following English, Chinese is the second most popular language used on the internet (Miniwatts Marketing Group, 2019).

Cybercrime literature in Chinese is limited, with most focusing on discussions relating to law and policy. Cybercrime, as considered within the Chinese cybercrime literature, is defined in ways that are similar to the English literature, though the Chinese government defines cybercriminal behaviour more broadly than western countries, including activities such as distributing pornography and spreading rumours as crimes under its cybersecurity law. Empirical research in Chinese, dealing with cyber-enabled crime, is emerging in academic research. Online fraud and telecommunication fraud are the most popular topics researched as these present a serious problem to Chinese societies. This section reviews the Chinese literature relating to cybercrime, especially the financial dimensions of cybercrime.

The first section shows the research methods used to conduct the review and locate relevant articles. The second section of the report gives an overview of government and private bodies involved in countering cybercrime. The third section provides the results from the review, highlighting what we know about the cybercrime ecosystem, types of cybercrime reviewed in the literature, motivation of cyberoffenders, proceeds of cybercrime, and responses to cybercrime. The last section introduces current laws adopted in Taiwan and China to combat cybercrime and regulate transactions related to cybercrime.

Methodology

This report focuses mainly on Chinese-language sources (both traditional and simplified Chinese). It systematically reviews the existing literature on criminal transactional methods in cyberspace conducted in the Chinese language. While the report uses mainly literature published in Chinese, English literature with a focus on cybercrime in China and Taiwan, is also reviewed to provide a comprehensive understanding of financial cybercrime and criminal financial transactions in cyberspace. Literature from various sources, including conceptual essays, policy analyses, white papers, book chapters, and journal articles are examined as well. Consistent with the English review, only articles, books, book chapters, and relevant reports that are accessible through our university system and that have been published in 2013 or afterwards are reviewed.

A key word search was first conducted using Google Scholar to capture a wide range of literature on illicit transactional methods in cybercrime. Google Scholar covers academic work and other grey literature that may not be captured in standard academic citation index databases, and it allows us to limit the searches to results in Chinese. We used similar keyword combinations as in the English review:

Main word	**Second word**
Cybercrime	Fraud □□□□
□□□□	Theft □□□□
□□□□	Money laundering □□□□
□□□□	Extortion□□□□
	Corruption □□□□

	Cryptocurrencies (□□□□□□□□)
	Capital movement/ transfer (□□□□)
	Disposing of proceeds of crime using online means□□□□□□□□□□□□□□□

Second, keyword searches were conducted on□□□□ (CNKI. Net), the largest database of scientific articles in simplified Chinese, and □□□□□□□ (Ariti Library), the largest database of scientific articles in traditional Chinese. We searched relevant Chinese cybercrime and criminology related journals using the same search terms as above. These included but were not limited to □□□□□ (*Journal of Criminology*), □□□□□□□ (*Crime and Criminal Justice International*), □□□□ (*Police Science Quarterly*), □□□□□□□□□□ (*Journal of Information, Technology and Society*), □□□□□ (*Legal System and Society*) and □□□□□□□□□□ (□□□□□) (*Journal of People's Public Security University of China (Social Sciences Edition)*).

Third, we conducted targeted searches among government agencies, think tanks, and non-profits in both Taiwan and China where Chinese is the only official language. The keyword searches were complemented with an examination of the work of recognised experts on illicit transactional methods in cyberspace and cybercrime in the Greater China region. Among the experts reviewed were □□ (Pi Yung), and □□□ (Ju Yunxi) in China and □□□ (Mon Weide) and □□□ (Chang Yaochung) in Taiwan.

The Chinese literature review resulted in the retention of 57 manuscripts – 15 from Taiwan and 42 from China – including academic journal articles, government reports, industry reports, and conference papers. Most of the papers are conceptual and theoretic pieces, discussing legal responses to cybercrime and cyber security. As some of the manuscripts are descriptive and/or similar to other manuscripts, not all of them are cited in this research. Empirical research is still rare in the Chinese literature. Also, most of the papers address telecommunication and online fraud, which has long been a serious crime issue, troubling both the Taiwanese and Chinese governments.

The State of Play in Chinese-speaking countries: China and Taiwan

This section provides an overview of the relevant cybercrime regulations and bodies involved in two major Chinese speaking countries/regions: China and Taiwan.

People's Republic of China (China)

Cybercrime has become a significant problem in China. Cybercrime in China is estimated to be valued in excess of USD $15.1 billion (100 billion Chinese yuan), and more than one third of all crime in China is believed to be cybercrime (An, 2017). According to Xinhua, the official state-run press agency of the People's Republic of China, China shutdown more than 4,000 websites and online accounts in an Internet clean-up campaign in 2018. In addition, more than 147,000 harmful online materials were removed by the end of August 2018. According to the Ministry of Public Security, Chinese authorities arrested more than 830,000 suspects and deleted more than 4 million illegal messages online. Most cases released by the Ministry related to financial cybercrime (Stanway, 2018).

Cybercrime

Although China's National Cyber Security Law was not published until 2017, China in earlier years had set up government agencies prioritising or dedicated to combating cybercrime. These include:

- the Central Cyberspace Affairs Commission (□□□□□□□□□□□□□),
- the Office of the Central Cyberspace Affairs Commission (□□□□□□□□□□),
- China's National Computer Emergency Response Team (CNCERT, □□□□□□□□□), and,
- the Office of Cyber Security of the Ministry of Public Security (□□□□□□□□□□).

- **Central Cyberspace Affairs Commission (□□□□□□□□□□□□□)**. The Central Cyberspace Affairs Commission, also called the Central Cybersecurity and Informatization Commission, is a permanent government body that was formed under the Central Committee of the Communist Party of China. Headed by President Xi Jinping and Primer Li Keqiang, the Central Cyberspace Affairs Commission is the main government agency to lead, formulate, and implement internet-related policy, including policies relating to cyber security, internet services, and internet censorship (including the great firewall). It was formerly known as the **Central Leading Group for Cybersecurity and Informatization** (□□□□□□□□□□□□□□), a taskforce established in 2014 to study cyberspace affairs. The **Leading Group** was restructured in 2018 into a permanent government agency, the **Central Cyberspace Affairs Commission,** as part of the reform of central government commissions.
- **Office of the Central Cyberspace Affairs Commission (□□□□□□□□□□).** The Office of the Central Cyberspace Affairs Commission, also known as the Cyberspace Administration of China (□□□□□□□□□□), acts as the executive arm of the Central Affairs Commission and answers directly to the Central Cyberspace Affairs

Commission. According to the National Cyber Security Law 2017, the Office of the Central Cyberspace Affairs Commission is the central agency that protects national cyber security and supervises relevant local government departments. The Office publishes the annual *China Statistical Report on Internet Development* and organises the World Internet Summit each year. The Office also manages a reporting centre which allows people to report illegal and unethical information online.

- **National Computer Emergency Response Team (□□□□□□□□□).** Established in 2001, the National Computer Emergency Response Team (CNCERT) is a non-profit and non-government organisation. CNCERT was set up to improve the nation's cybersecurity posture and to protect critical information infrastructure from cyberattacks. It proactively detects and monitors cyber incidents and threats, especially for critical, national infrastructure, such as energy, telecommunications, water, and electricity. It coordinates with key government and non-government agencies to handle significant cyber security incidents jointly on a 24/7 basis. It publishes alerts concerning vulnerabilities and threats and provides support to improve computer and network security in China.

- **Office of Cyber Security of the Ministry of Public Security (□□□□□□□□□□).** The Office of Cyber Security of the Ministry of Public Security is the leading law enforcement agency specialising in cybercrime investigation. Apart from cybercrime investigation, in collaboration with certain Internet Service Providers and website managers, the Ministry of Public Security provides cyber police to conduct online patrols. In 2018, the Rules on Supervision and Inspection of Internet Security (□□□□□□□□□□□□□□□) were issued by the Ministry of Public Security. These rules allow cyber police to supervise and inspect Internet Service Providers and “unit utilizing networks” (such as websites) so that they comply with their cyber security obligations.

Financial Crime

The People’s Bank of China (PBC), which is the central bank of China, is responsible for regulating financial institutions. Although the PBC is a department of the State Council, it possesses a high level of independence when it comes to conducting its duty under the Law of the People’s Republic of China. The PBC hosts the Financial Intelligence Unit which consists of the Anti-Money Laundering Bureau, the China Anti-Money Laundering Monitoring and Analysis Centre, and 36 PBC branches in provinces. The Economic Crime Investigation Department under the Ministry of Public Security leads the investigation of money laundering and terrorism financing activities. Apart from the PBC, the **Anti-Money Laundering Joint Ministerial Conference** was established by the State Council of the People’s Republic of China to build better collaboration among government departments on anti-money laundering investigations.

- **The Anti-Money Laundering Joint Ministerial Conference (□□□□□□□□□□□).** The Anti-Money Laundering Joint Ministerial Conference (AMLJMC) was established in 2002 to build effective collaboration among departments in combating money laundering in China. The AMLJMC involves 23 government departments, including the Supreme People’s Court, the Ministry of State Security, the General Administration of Customs, the State Administration of Taxation, the Ministry of Justice, the Ministry of Foreign Affairs, and the National Supervisory Commission. It is coordinated by the People’s Bank of China and is the highest anti-money laundering and counter-terrorism financing body. It aims to strengthen anti-money laundering related policy and to promote collaboration on the investigation of money laundering.

In terms of international collaboration, China is a member of the Financial Action Task Force (FATF) and is a founding member of the Eurasian Group on Combating Money Laundering and financing of terrorism.

Taiwan

Cybercrime

Taiwan, due to its special political situation, where its sovereignty is contested by China, which views Taiwan as a province of China, suffers severe cyberattacks and cybercrime, especially from hackers in mainland China. It was reported in 2018 that Taiwanese Government agencies, as a whole, received over 20 million cyberattacks every month (Gu, 2018). While the attacks are going through bot-infected computers as springboards, it is believed that most of the attacks originate from China.

Cybercrime and cyber security incidents are causing considerable economic damage to Taiwan. Although a 2018 Microsoft report on cyber security in the Asia-Pacific region indicated that cyberattacks had cost Taiwan NTD 81 billion (approximately USD $2.66 billion), most Taiwanese citizens still do not have good cyber security awareness (Chang, 2018). The Taiwanese Government has invested greatly to improve cyber security through hardening the network system and providing cyber security training. And in 2017, President Tsai Ing-Wen declared that ‘cybersecurity is national security’, showing the government’s determination to build cyber capacity and improve online safety.

At the same time, Taiwanese law enforcement agencies play a significant role in the fight against transnational cybercrime. The Investigation Bureau under the Ministry of Justice participated in an international consortium of law enforcement, commercial, academic, and private organizations from 31 countries to take down the Avalanche botnet, a platform to distribute malicious software and to send phishing emails, in 2016. Agencies in Taiwan charged with responding to cybercrime issues include:

- **National Information and Communication Security Task Force (□□□□□□□□□).** The National Information and Communication Security Task Force (NIST) was established in 2011 to promote policies on national information and communication (IC) security, expedite the construction of a safe national IC environment and boost national competitiveness. [68] Led by the Vice Premier of the Executive Yuan, the NIST is responsible for advice on IC security policies, incident report process, and other IC security programs. The NIST is also responsible for coordinating and supervising inter-ministry cyber security efforts and implementing other cyber security related matters assigned by the Executive Yuan. The Department of Cyber Security under the NIST assists the NIST to draft and promote policies. It also audits the implementation of computer incident emergency reporting and responses and supervises cyber security education.
- **Ministry of Justice Investigation Bureau (□□□□□□).** The Crime Investigation Bureau under the Ministry of Justice (MJIB) is in charge of cybercrime and money laundering investigations. It actively collects and monitors cyber security threat information in Taiwan and promptly notifies government agencies and other important organisations about the threat and ways to prevent it. The MJIB Cyber Forensic Laboratory was established in 2006 to assist in search and seizure of digital evidence. The Laboratory also provides service to judges and prosecutors in recovering and auditing evidence, as well as providing forensic reports.
- **Crime Investigation Bureau, The National Police Agency, Ministry of the Interior (□□□□□□).** The Crime Investigation Bureau under the National Police Agency, Ministry of the Interior, is another agency investigating cybercrime. Its responsibilities are similar to those of the MJIB. Specifically, the Ninth Police Brigade specialises in investigating technology crime and cybercrime.
- **Taiwan Computer Emergency Response Team/ Coordination Center (□□□□□□□□□□□□□□□).** The Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC) is a non-profit, non-government organisation. Established in 1998, TWCERT/CC aims to promote cyber security incident reporting and coordinates the sharing of cyber security incidents reports and cyber security education. It also

facilitates exchanges of intelligence, both nationally and internationally, and promotes public and private collaboration on cyber security issues.

- **Taiwan Information Security Center (□□□□□□□□□□□).** The Taiwan Information Security Center (TWISC) was established in 2005 with funding support from Taiwan’s National Science Council. It was established to provide education and professional training on cyber security. It also connects government, industry, and academia to promote collaborative research and develop new cyber security standards.

Financial Crime

In Taiwan, the Central Bank of Taiwan and the Financial Supervisory Commission are the two main authorities that regulate and audit financial institutions. The Central Bank used to be the only regulator but some of its power was shifted to the Financial Supervisory Commission with the latter’s establishment in July 2004. Both are responsible for anti-money laundering and countering terrorism financing (AML/CTF). In order to build better collaboration on AML/CTF, the Anti-Money Laundering Office was established under the Executive Yuan.

- **Anti-Money Laundering Office, Executive Yuan (□□□□□□□□□).** As a member of the Asia/Pacific Group on Anti-Money Laundering (APG), Taiwan closely follows international rules and standards on AML/CTF. The Anti-Money Laundering Office (AML Office) was established in 2017 in response to the APG which requires its members to establish a national coordination mechanism. The AML Office, in collaboration with the public and private sectors, reviews national policies on AML/CTF and monitors and prepares for the APG mutual evaluation.
- **The Financial Supervisory Commission (□□□□□□□).** The Financial Supervisory Commission (FSC), established in 2004, is responsible for the development, supervision, regulation, and examination of financial markets and financial service enterprises in Taiwan. The financial industry, including banks, securities and futures exchanges, and insurance companies, is under the supervision of the FSC. The FSC is also the regulator and auditor of AML/CTF in the financial industry.
- **The Central Bank (□□□□).** The Central Bank of Taiwan is an independent agency. The Governor of the bank is appointed by Parliament for a term of five years. The core responsibilities of the Central Bank of Taiwan include monetary management, foreign exchange management, and currency issuance. While some of the auditing work has been shifted to the Financial Supervisory Commission, the Central Bank is still in charge of auditing financial institutions, relating to currency, foreign exchange, and credit.

Review of the Chinese Cybercrime Literature

Cybercrime has become a major concern for both the Chinese and Taiwanese governments, particularly as the internet penetration rate in both countries has increased. Despite the volume of resources devoted to this area, the Chinese cybercrime literature remains scarce in both English and Chinese (Trend Micro 2016). One problem that contributes to the lack of Chinese-language research is state censorship, where research that touches on sordid aspects of cybercrime may be declared indecent.

We have organised the available literature into four main sections. The first section focuses on the ecosystem of cybercrime, comprising the character of cybercrime and the development of the internet dark industry (□□□□□, illegal internet industry, not to be confused with darkweb activities) in China. The second section focuses on the motivations of cyberoffenders, with a focus on studies developing typologies of hacker motivations and telecommunication fraud. The third section examines studies that have assessed the financial transactions of cyberoffenders, with a focus on how cyber criminals monetise their crimes. The fourth section outlines government and private sector responses to countering cybercrime.

The Chinese Internet Dark Industry: China's Ecosystem of Cybercrime

With regards to the ecosystem of cybercrime, Yu (2018) reviewed the history of cybercrime in China. He divided the development of cybercrime in China into pre-internet and post-internet stages. He argues that cybercrime in China evolved from computer crime where the computer is just a mediator of traditional crime (e.g. intellectual property theft). The existence of computers does not contribute much to the event of the crime. But now we are in an era in which cybercrime is 'spatialised' (□□□). That is, cybercrime is no longer a one-to-one crime. Large scale cybercrime is occurring, and crime syndicates are more likely than individuals to be the perpetrators of cybercrime.

At the Forum of the National Internet Security and Informationalization in 2018, President Xi Jinping of the People's Republic of China emphasised the importance of striking hard against hackers, telecommunication and online fraud, and criminal behaviour that infringes upon individuals' privacy. It is also important to cut the internet crime benefit chain and enforce the law strictly to suppress cybercrime and deter potential cybercriminals from conducting cybercrime (Beijing Haidian People's Procuratorate, 2019). Beijing Haidian People's Procuratorate, a district prosecutor's office in Beijing, analysed 450 cases that the Procuratorate had received from September 2016 to the end of 2018, and summarised the character of cybercrime and cybercriminals as follows (2019: 2-5):

1. **Cybercriminals tend to be young males, with low education qualifications**: 77% of the cybercriminals in these cases were male; 37.58% of the criminals were born between 1990-1999 (age 20-30), and 48.12% of the cybercriminals were born between 1980-1989. In terms of education qualification, more than 60% had a highest education qualification of junior high school or below.
2. **Cybercrime is not limited to traditional territories**: Most of the cybercrimes in the cases analysed were cross-jurisdictional. Co-offenders might not necessarily have known each other in person, and they would communicate with each other through online forums and chat groups such as QQ and WeChat.
3. **Cybercrime is a business:** Cybercrime is becoming an “industry chain” (□□□□□) called “the internet dark industry chain” (□□□□□□□). The industry chain can be divided into streams: up-stream, mid-stream, and down-stream. Cybercriminals in the upstream category provide hacking tools, such as Trojans or viruses and/or provide online platforms for cybercriminals in the lower stream to set up phishing websites. They also attract victims to install a trojan in order to gain control of the victims’ computers. These computers, controlled by the hacker, then become “zombie computers” (bot-infected computers) and are used by the criminals in the mid-stream as springboards to commit cybercrime and to launch cyberattacks. Cybercriminals in the down-stream category are those who monetise cybercrime; for example, they are the ones who sell the hacking tools and teach others how to use the tools and withdraw money using fake credit cards.
4. **Most large-scale cybercrime is done by teams:** It is becoming difficult for individuals to commit large scale cybercrime on their own. Online fraud, for example, involves such as crime syndicates, legitimate companies, and money mules with clear divisions of labour.
5. **Cybercriminals target a large number of victims though victims have relatively small losses:** For online scams, cybercriminals do not have specific targets. They send out phishing or scam emails to the public and wait for them to reply. Although the loss incurred by the individual victim is small, the large number of victims makes the scam profitable. It is quite normal to see online fraud involving tens of millions of RMB in China.
6. **Chinese cybercrime is globalised:** Most of the servers used for cybercrime are located outside China. Cybercriminals usually rent servers located in places outside

China, such as in the US, Spain, or Kenya. As a result, crime investigation is difficult.

According to Yuan et al (2018), the internet dark industry (or illegal internet industry) refers the illegal online industries that use information technology as a tool and the internet as a medium to gain illegal financial benefit. It includes career hackers and their activities in an ‘up-stream’ sector; career middlemen who sell, promote and use these hacking skills in a ‘mid-stream’ sector; and people who monetise cybercrime by selling the stolen personal data, withdrawing money from ATMs (online fraud cases) and other similar activities in a ‘down-stream’ sector. As more mid-stream actors gain purchase on cybercrime, the illegal online industry develops into multi-sections, multi-layers, and marketized criminal activities. Another consequence is , as Yuan et al (2018) argue, the way in which cybercrime is configured is moving away from a ‘chain’ that connects upstream, middle-stream, and downstream actors and processes in sequence and is becoming an illegal internet industry ‘network’ with more players joining the industry and better division of labour that is available on demand.

Based on its application and the cybercrime involved, the internet dark industry can be categorised into seven categories: the information theft industry chain, the hacker training industry chain, the online gaming industry chain (to earn or steal virtual money and/or treasure), the malicious advertisement industry chain, the SPAM industry chain, the ransomware/online extortion industry chain, and the web spoofing industry chain (Liu, 2014; Guo, 2015; Yuan et al, 2018). Song (2013) used the term ‘Internet Black Society’ to describe the dark industry chain.

There is no specific academic literature in the Chinese language that examines the cybercrime ecosystem in Taiwan. However, the official statistics released by the Taiwanese government show that, in 2018, more than 40% of cybercrime suspects were under the age of 30 and about 30% of cybercrime suspects were aged between 30-39. Between 2006 and 2015, the number of cybercrime cases decreased. And, unlike China, the majority of cybercriminals (suspects) in Taiwan are well-educated, with more than 75% having a senior high school diploma (CIB, 2019).

Cyberoffender Motivations and Typologies

The China Computer Emergency Response Team (CNCERT) publishes the China Cyber Security Report (□□□□□□□□□□□) annually. In its 2018 report, CNCERT indicated that China is under more frequent advanced persistent threat (APT) attacks. Industries, including health, media, and telecommunication, are usually the target of the APT attacks and the modus operandi is becoming more sophisticated. With the prevalence of cloud computing, there has been a dramatic increase in attacks directed at the cloud system in China. Denial of Service attacks (DDoS), installation of backdoor, and web spoofing are all on the increase and are the main types of cyberattacks towards the cloud computing system. The report also pointed out that there is an increase in attacks towards Supervisory Control and Data Acquisition (SCADA), a control system used by industrial organisations to maintain the efficiency of data processing. Cyber-enabled crimes, such as online investment, online dating, online lending/loan, and data theft, are also on the increase and are causing significant financial damage to individuals in China.

The Taiwan Computer Emergency Response Team also publishes an annual cyber security report, based on their own monitoring of the system and analysis of incidents reported to them in the previous year. In its 2018 report, TWCERT noted that around 20% of all cyberattacks targeted the financial services industry. These included hacking into the SWIFT system and using ransomware or phishing emails to steal personal information and passwords. The report also noted an increase in cyberattacks towards other critical infrastructure, such as transportation and government agencies. It specified key cybercrime and cyber security incidents that had happened in Taiwan and found that cybercriminals had embedded a cryptomining program on the webpages they were managing. The mining program was then installed onto any system/computer that visited the webpage, making the visitor work as a miner for the person controlling the program. In addition, the report found an increase in mobile spying apps which use the victim’s mobile phone to record sound as well as keystrokes. TWCERT (2018) analysed the cases collected and suggested that hacking has become sophisticated with a clear division of labour within hacking groups, and with improved and upgraded hacking tools. These findings align with the situation in China.

The majority of cyberoffenders in China pursue fiat money (Xu, 2014). Telecommunication fraud and online scams are the most popular types of cybercrime in both Taiwan and China and are the most discussed in the academic literature. This focus may reflect the prevalence of online scams or may reflect how financial cybercrime attracts more research interest. Ma (2017), using official data from an unnamed province in China, pointed out that telecommunication fraud caused the province to lose more than 122 million RMB (17.34 million USD) in the third quarter of 2017.

Cybercriminals use various modus operandi to conduct fraud. According to Ma (2017), common modus operandi include offenders pretending to be prosecutors or acquaintances of the victim to establish trust which they then use to ask victims to transfer money. Other scams involve offenders pretending to be online salespeople for online shopping sites telling the victims that the transaction failed and instructing them to pay again using a different means, or pretending to be someone who was willing to pay a large amount of money for a sperm donor but asking the victims to pay fees to guarantee the donation. In some cases, offenders use violence to coerce their victims by pretending to be gangsters and threaten victims if they refuse to pay. Some offenders hijack Quick Response (QR) codes in payment terminals (Tao 2017, Yeung 2017, Yu, Su, and Li 2017). QR codes have significantly cut into cash and card payments since 2014. One common scam involves the offender placing embedded codes to redirect payments from the payee to the scammers' accounts rather than the merchants' accounts (Li, 2017; Yu, Su and Li, 2017; Yueng, 2017).

Tei (2017) analysed Hainan Province in China and found that most of the suspects involved in fraud processes were aged between 18-35 and that, although most of the suspects were male a substantial percentage were female. Third parties were usually hired as money mules to get or transfer money. Although most of the members did not know each other, they worked as a team through mobile chat groups such as WeChat or QQ, despite privacy concerns. Zhao (2017) focused on online fraud targeting high school students. He argued that the schools are not protecting students' personal data; as a result, cybercriminals can access students' personal information easily. With this information, scammers can accomplish their scams easily by exploiting the trust they built with the students leveraging the personal data they acquired.

In addition, there have existed underground, darkweb marketplaces that have sold software and other tools to facilitate cybercrime and mobile phone crime (Gu 2014, Trend Micro 2016). However, it appears that these marketplaces are not common, perhaps due to difficulties of access to darkweb protocols caused by regulation or censorship, and it is unclear to what extent these marketplaces have managed to sustain their presence over time. One observation of a Chinese darkweb forum, '□□□□□□,' where the marketplace ceased operation suddenly, was unable to determine displacement or reinitialization of this forum in an alternative space (Wong 2017).

Proceeds of cybercrime

Most of the Chinese literature mentions the proceeds of cybercrime, without going into great detail. Li, Li and Wang (2016) mention that the traditional bank is still a popular target for cyberoffenders. Fake accounts are usually created and used by telecommunication fraud and online scam syndicates. Using personal information stolen or bought online, cyberoffenders can easily open new bank accounts. When cyberoffenders apply to open a new bank account, they find someone who resembles the person who is on the stolen Chinese identity card being used to open the account. The offenders usually come to the bank as a group of two or three people and, while the clerk is processing the application, they pretend to be busy on their phones so that their faces will not be recorded by the CCTV. They are usually very familiar with the application process and readily recite the stolen identity card's information, such as ID card number, address, and other information on the ID card. They usually choose small branches where the governance might not be as strong as at the main branches. They might threaten to report the clerk if the clerk asks too many questions or senses that something may be wrong. However, even when the cyberoffenders are well prepared, a clerk may question their identity especially if their accent does not match that common to the region noted on the card. At the same time, the bank's merit-based performance evaluation creates a vulnerability as the clerk strives to meet a monthly quota of new customers. Accordingly, it is important to create a better governance system and better training for bank clerks on the frontline. (Fan and Wang 2017; Li, 2014; Li et al, 2016; Tei, 2017). Tei (2017) notes that once the money is transferred into these fake accounts, criminals wire it out directly to several other accounts in other provinces and withdraw the money from ATMs or spend the money at shops with point of sale machines.

One of the main reasons ransomware has become prevalent globally is that it uses the Tor system and asks victims to pay in bitcoin or other cryptocurrencies. The Tor system and cryptocurrencies make crime investigation difficult, especially when it comes to tracing the money flow. However, cryptocurrencies are not popular in China, since Tor and bitcoin are banned in China. Sun and Du (2017) argue that this ban might explain why most of the earlier ransomware attacks were not based in China. However, in 2016, the first ransomware, Ransom_SHUNJIN.A, was seen in simplified Chinese, explaining how to escape the "E Great Wall" (the internet censorship of China) (Sun and Du, 2017). There are also services provided to victims in China to pay for the ransom in bitcoin.

Research on money laundering using cryptocurrency has emerged in the past couple of years. Both Jihong Shi (2018) and Xiuxia Shi (2017) discuss how cryptocurrency might be used as a tool for money laundering. However, both studies do not touch on real cases. Instead, they focus on concepts and the lack of regulation in this area in both

Taiwan and China. Shi (2017) argues that decentralisation, secrecy, and anonymity make virtual currency (including cryptocurrency) a good currency for money laundering. There is no identity check to open an account on a cryptocurrency exchange and there is no central management mechanism. Also, there are multiple ways to get virtual currencies, such as through money mules, online payment, third party payment, pre-paid card, cash, other virtual currencies or even through mining (Shi, 2017). These all make it difficult for crime investigation. The lack of professional knowledge among law enforcers on virtual currencies and law enforcement’s low capacity to collect digital evidence all make virtual currency a good choice for money laundering. In 2016, online scammers were already using bitcoin and OneCoin – a coin offering that turned out to be a Ponzi scheme (Yang 2018) – to launder their money.

Mobile payment and third-party payment systems, on the other hand, are the most popular payment systems use by cyberoffenders. Stored-value cards, such as credit for online gaming, cash vouchers for online shopping (e.g. Tien Mao voucher, a voucher issued by the largest online shopping company TaoBao), and credit for mobiles (e.g. QQ coin, a credit system used by QQ, an instant messaging app) are popular among cybercriminals. Third-party payment through WeChat pay, a payment mechanism from Tencent, and Alipay, a payment mechanism from Alibaba, are also popular due to their semi-anonymous character. Cybercriminals use fake email addresses and chat accounts to ask victims to pay money through these channels (Beijing Haidian People’s Procuratorate, 2019; Sun and Du, 2017).

Luo (2018) indicated that it has become difficult to build links between payees and payers if transactions are made using mobile payment or third-party payment systems. With a traditional payment, banks can see the money flow. However, third-party payments and mobile payments have broken this rule by inserting a middleman. As a result, banks can only see money being transferred to or from service providers. At the same time, it is very easy for individuals to open an account on the mobile or third-party payment system. The requirements and the proving process for opening a mobile account or third-party account are not as rigid as opening a bank account. To attract more clients, some mobile account or third-party account companies do not even have a review process, which creates opportunities for cybercriminals.

There are also companies that provide services to clients dealing with large amounts of money. Since payments made through mobile payment or third-party payment systems face value limits per transaction. For example, WeChat pay has a limit of USD 1,000 per transaction and not exceeding USD 10,000 per month per account. However, some companies provide services to facilitate large transactions by hiring money mules and pay them a small commission to circumvent these limits. Luo (2019) indicated that some companies have more than 40,000 mules, many of whom launder “dirty money” through a fake online shopping process.

Responses to Cybercrime

Cybercrime investigation and prosecution is a common topic discussed in the Chinese literature. There is a consensus that, although government needs to invest more resources in combating cybercrime, contributions from the private sector and individuals are also crucial. That is, combating cybercrime is no longer an effort that can be done by only law enforcement agencies. With the private sector holding most of the information, there is a need to build a feasible public and private collaboration against cybercrime (Chang, 2012).

Fan and Wang (2017) argue that it is still very difficult to collect digital evidence pertaining to telecommunication fraud and online scams. Because it usually takes a long time for crime investigators to collect relevant evidence, organised crime syndicates destroy or delete most of the crucial evidence once they learn that they are under investigation. Cross-jurisdiction and cross-border issues make the collection of evidence even more difficult. In addition to being time consuming, police from other jurisdictions are unwilling to help and usually hinder the process of the investigation (Fan and Wang, 2017; Lo, 2018; Mon, 2019; Yu, 2018).

Xu (2014) and Ma (2018) also discuss the multi-jurisdiction issue. Ma (2018) argues, as the fraudulent information is spread over the internet platform and by email, it is hard to decide “the place where the crime happens” and “the place where the crime results”. As a result, it is difficult to decide which jurisdiction should take charge of the case. Although a new directive has given a higher authority the power to decide which police agency should be responsible, it usually takes a long time for this decision to be made. Also, when cases are sent to the Procuratorate, those there might not agree with the initial decision to prosecute, thereby undermining the original investigation.

The cross-border nature of cybercrime makes cybercrime investigation even more difficult. Without efficient and close collaboration between governments in crime investigation, exchange of crime information and evidence, as well as extradition processes, cybercriminals face a low risk of arrest and prosecution. Chang (2012) argues that the special political situation between Taiwan and China gives cybercriminals an opportunity to conduct cross-border crime. Also, inconsistency of laws and the lack of extradition rules hinder the investigation of cross-border cybercrimes.

Both Taiwan and China are building new task forces and divisions to fight cybercrime. As mentioned earlier, special divisions have been added to the police agencies, crime investigation bureaus, and the Procuratorate. For example, Beijing Haidian People’s Procuratorate has established a professional department to target cybercrime. This department not only trains the prosecutors in the Procuratorate, but it also creates a platform for collaboration with higher education institutions in the district. External experts have been invited to provide legal opinions on cybercrime related cases, and this has contributed to some success in prosecuting cybercriminals (Beijing Haidian People’s Procuratorate, 2019).

In addition to strengthening the capacity of the government, the private sector plays an important role in responding to cybercrime. Li, Li and Wang (2017) and Yu (2011) emphasised the importance of banks double checking the identity of their clients and making sure that new accounts opened are not fake accounts and/or are not being used as mules. Adequate preventative measures need to be adopted by banks to detect suspicious transactions and report them to the authorities when they believe the transactions are related to crime. Liu (2014) notes that the internet company Tencent collaborated with the police to locate the IP of cybercriminals which led to successful investigations. As most of the transactions are through third party payment and online payment systems, the literature argues that these companies need to take greater measures to prevent their platforms from being used by cybercriminals.

Regulations vis-à-vis Cybercrime

China

Legal Regulations

Criminal Law (□□□□□□□□□)

China’s cybercrime laws are contained in the *Criminal Law* of the People’s Republic of China 1979. Articles 285 and 286 were added in 2009 to regulate offences against the confidentiality, integrity, and availability of computer data and systems. Also, Article 287 regulates against committing financial crime using a computer. However, while Article 285 regulates illegal access to computer systems and misuse of devices, this article applies only to crime towards computer systems with information concerning state affairs, construction of defence facilities, and sophisticated science and technology. Article 286 regulates data interference and system interference.

Cybersecurity Law (□□□□□□□□□□□)

The Cybersecurity Law was passed in 2016 and came into force in June 2017. It was formulated to ensure cybersecurity and to protect internet sovereignty, national security, public interest, and the lawful right of individuals and organisations, and to promote healthy development of informationization of the economy and society (Article 1). The Law gives the State the power to take measures for monitoring, preventing, and handling cyber security risks and threats and to protect critical information infrastructure from cyberattack. The Law outlines the responsibilities of the government, internet service providers, and individuals in maintaining cybersecurity. Article 12 protects citizens by raising the security of network services. It prohibits any individual or organisation from using the internet to commit cybercrimes that endanger national security, honour, and interests. These include crimes, such as terrorism, dissemination of hate speech, messages relating to the separation of the country or damage to the unification of the country, violence, pornography, and spreading rumours in order to disrupt the economic or social order. Article 21 establishes a Multi-Level Protection System (MLPS) for cybersecurity.

- **Law of the People’s Republic of China on Anti-money Laundering (□□□□□□□□□□□)**

> The Law of the People’s Republic of China on Anti-money Laundering (AML Law) was formulated to prevent any money laundering activities for the purpose of concealing or disguising the sources and nature of criminal proceeds generated from drug-related crime, organised crime of any gang, terrorism, smuggling, corruption or bribery, disrupting of financial order, and financial fraud (Articles 1 and 2). Both financial institutions established within the territory of China and special non-financial institutions, including real estate agents, dealers or exchanges of precious metal, accounting and law firms which manage client funds or buying and selling estates, are responsible for preventing anti-money laundering by adopting relevant measures according to the Law. The AML Law also applies in the supervision of any fund suspected of being involved in terrorism activities.

- **Counter-Terrorism Law of the People’s Republic of China (□□□□□□□□□□□□□)**

> The Counter-Terrorism (CT) Law of the People’s Republic of China was passed in December 2015 and came into force on January 1, 2016. The main purposes of the CT Law are to prevent and punish terrorist activities, as well as to strengthen counter terrorism capacity. According to Article 3 of the CT Law, terrorist activities include activities of a terrorist nature, such as organising, planning, preparing for or carrying out conduct that causes harm to society; advocating or unlawfully possessing items for terrorism or inciting others to commit terrorist acts; organising, leading, or participating in a terrorist organization; providing information, capital, funding, labour, technology or a venue to support, assist or facilitate terrorist organisations, terrorist personnel or the commission of terrorist activities. Telecommunication and Internet Service Providers are required to monitor the content posted online and provide technical assistance to prevent the dissemination of messages relating to terrorism and extremism. The administrative departments of the State Council responsible for combating money laundering are also responsible for combating financing suspected to be related to terrorism.

Financial Regulations

China has several regulations and decisions on anti-money laundering and counter terrorism financing (AML/CTF). The Anti-Money Laundering Law is the fundamental law dealing with AML/CTF in China. Although the AML Law regulates “specific non-financial organisations,” such as real estate agents, dealers or exchanges of precious metal, accounting and law firms which manage client funds or buying and selling estates, it has been criticised for not being able to handle new types of money laundering through online payment or third-party payment systems (Ma, 2018).

- **Regulation on Internet Financial Institutions against Money Laundering and Terrorism Financing (□□□□□□□□□□□□□□□□□□□□□□□□□□)**

> In addition to China’s Anti-Money Laundering Law, Anti-Terrorism Law and the Law of the People’s Bank of China, the Regulation on Internet Financial Institutions against Money Laundering and Terrorism Financing came into force in January 2019. The Regulation aims to close a gap by putting anti-money laundering and counter-terrorism financial responsibilities onto internet financing institutions, including internet lenders, internet payment providers, internet financing information intermediaries, equity crowdfunding platforms, online fund sellers, insurance and trust platforms, and internet consumer finance companies (Article 2). The People’s Bank of China has been authorised to establish an anti-

> money laundering auditing and monitoring centre and a monitoring platform to receive and analyse block transactions and suspicious transaction reports. The platform is designed to be managed and maintained by the Internet Financial Association which also has the responsibility to coordinate with its members to come up with self-regulation to promote AML/CTF.

Taiwan

Legal Regulations

- **Criminal Law (□□□□□□)**

> Although Taiwan is not eligible to be a signatory of the Budapest Convention due to its special political situation, its *Criminal Code* was amended in 2003 to regulate cybercrime consistent with the Convention by the addition of Chapter 36 Offenses Against Computer Security (Chang, 2012). There are six articles (Articles 358 to 363) in this Chapter, covering illegal access, illegal interception, data interference, system interference, and misuse of devices. In the context of Article 358, intentional access to a computer, by using another's password without right or by the act of circumventing protective measures or by discovering or exploiting loopholes in another computer system, is punishable by up to three years in prison and/or a fine of up to NT$100,000. Article 359 regulates unauthorised acquisition, deletion, or alteration of electromagnet records of another's computer. System interference is regulated in Article 360 to protect the Internet from being paralysed by a Distributed Denial of Service or equivalent attacks. Article 362 focuses on the offence of the creation of computer programmes specifically for the perpetration of crime. Illegal interception is regulated in the *Communication Protection and Surveillance Act* which provides that illegal interception of another's communication can be punished by up to five years in prison. Currently, there is doubt over whether the *Communication Protection and Surveillance Act* applies to the regulation of only illegal interception by government agencies; a broader interpretation is supported by Taiwan's Ministry of Justice which asserts that this Act applies to illegal interception by non-government organizations or individuals as well.

- ***Money Laundering Control Act* (□□□□□)**

> The *Money Laundering Control Act* (MLCA) was first promulgated in 1996 and amendments were promulgated in November 2018. The amendments of the MLCA were designed to meet the recommendations made by the Financial Action Task

> Force on Money Laundering. Similar to the ML Law of China, the MLCA regulates both financial and designated non-financial institutions and personnel, including jewellery businesses, land administration agencies, real estate agencies, lawyers, notaries, accountants, trust and company service providers, and other businesses or professionals with the characteristics of their operation or transaction mode likely to be involved in money laundering (Article 5). Enterprises handling financial leasing, virtual currency platforms and transactions were added as financial institutions and covered by the regulation.

- **Counter-Terrorism Financing Act (□□□□□)**

> Taiwan does not have a counter-terrorism law. Instead, the *Counter-terrorism Financing Act* (CTFA) was promulgated and came into force in November 2018 to prevent and suppress the financing of terrorist acts, terrorist organisations, and personnel. According to CTFA, the Executive Yuan is the authority for counter terrorist financing. A Terrorist Financing Review Committee was established in 2017 by the Executive Yuan to review proposals of listing or delisting individuals or legal personnel or entities in a sanctions list.

Financial Regulations

Directives and self-regulation were introduced to meet the requirement of the MCLA and CTFA. For example, the Directions Governing Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business, Electronic Payment Institutions and Electronic Stored Value Card Issuers (□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□) were published in 2017 to “strengthen the anti-money laundering and countering terrorism financing (AML/CTF) regime of the Republic of China (R.O.C.), and to enhance the soundness of the internal control and internal audit system of the banking business, electronic payment institutions and electronic stored value card issuers”(Article 1). The Banks Association, Insurance Association, and other financial industry associations have all published guidelines to regulate their members against financing terrorism.

Conclusion

This section reviewed Chinese literature on cybercrime and criminal finance transactions in cyberspace. Although limited to Chinese literature on these issues, we see there has been an increase in cybercriminal activities using new technology to conduct crime and to monetise crime. Financial motivation is still the dominant purpose of cybercrime. Facilitated by the development of information and communication technologies, telecommunication fraud and online scams are now easily done in a cross-jurisdiction and cross-border manner. The barriers that exist in cross-border and cross-jurisdictional crimes make crime investigation and prosecution difficult. The special political situation between Taiwan and China makes the situation even worse.

As argued by academics and practitioners in China, cybercrime has developed into a dark industry chain. There is a clear division of labour, and monetising the crime is part of the industry chain. The use of third-party payment and online payment systems by cybercriminals to launder money through online shopping, online lending, or online gambling is becoming prevalent. As a result, this emerging area is less regulated than the traditional banking system. With regards to cryptomarket and cryptocurrency, there are only a couple of papers addressing money laundering and bitcoin which might be a reflection of the fact that China has a strict internet censorship regime that has banned the use of the cryptomarket.

This report also reviewed regulatory institutions in both Taiwan and China. Both governments are putting more resources and effort into building better regulations and institutions to govern cyber space. Law enforcement agencies are also strengthening their cybercrime prevention and investigation capacities. However, with the quick evolution of the technology, new opportunities are created and are used by cybercriminals. There is a need for the government to review its laws and regulations regularly to make sure they are up to date. There is also a need to provide regular training to law enforcers so that they can update their cybercrime knowledge and learn new methods to combat cybercrime.

Last, but not least, cybercrime remains under-researched in Chinese societies. In order to understand better the cybercrime situation in Chinese societies as well as how criminal financial transactions happen in cyberspace in China and Taiwan, more empirical research into the area is necessary. Incentives should be put in place to encourage more academics to research this multi-disciplinary area.

Works Cited

An, A. 2017. “Chinese cybercriminals develop lucrative hacking services.” *McAfee*, 23 December, 2017. Accessed 6 August 2019. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/chinese-cybercriminals-develop-lucrative-hacking-services/.

Beijing Haidian People’s Procuratorate. 2019. “Whitepaper on protecting internet security through criminal justice.” Beijing Haidian People’s Procuratorate.

Chang, LYC. 2012. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar.

Chang Tingyu. 2018. “tai wan yin ‘hai ke gong ji ‘ nian sun 8100 yi” [Cyber attacks had caused Taiwan a total loss of 810 billion], *Storm Media*, 12 June 2018. Accessed 12 September 2019https://www.storm.mg/lifestyle/448195

Crime Investigation Bureau (CIB). *Analysis of cybercrime*. Accessed 10 October 2019https://www.cib.gov.tw/Upload/Files/5699.pdf.

CNCERT. 2019.” 2018 China Cyber Security Report”. *Beijing: People’s Post and Telecommunication Press*.

CNNIC. 2019. *Statistical report on Internet Development in China*. Beijing: CNNIC.

Fan Yuqin and Wang Panpan. 2017. “Dianxin wangluo zhapian fanzui anjian shencha daibu de xianzhuang fenxi” [An analysis on current crime investigation on telecommuting and internet fraud], *Fazhi yu Shehu*i 11: 100-110.

Gu, L. 2014. *The Mobile Cybercriminal Underground Market in China*. *CyberCriminal Underground Economy Series*. Irving, Texas: Trend Micro.

Gu Qang. 2018. “Gong bu men zao wang gong mei yue yu 2 qian wan ci, duo shu lai zi zhong guo” [More than 20 million cyber attacks were launched towards government agencies, mainly from China], *Technews*, 5 April 2018. Accessed 10 August 2019https://technews.tw/2018/04/05/china-attack-tw-gov-internet-20-million-times-per-month/

Guo, Rui. 2015. “Wang luo hei se chan ye lian: fan zui zu zhi de “hu lian wang +”” [Network black industry chain “Internet Plus” of criminal organisation]. Xin xi An Quan, 6(2015): 3-5.

Hu Shuqi. 2018. “Zushou ‘jiangshi wangluo’ kongzhiquan hangwei de xingfa sisuo”[A thought on renting or selling botnets]. *Xinwen Qianshao* 3, (2018): 34.

Li Xiao, Liu Junqi and Fan Mingxiang. 2017. “WannaCry lesuo bingdu yufang ji yingdui celue yanjiu” [Combating Wannacry: Prvention and countermeasures]. *Diannao Zhishi yu jishu: Xueshu jiaoliu* 13, no. 7: 19-20.

Liu Qi. 2014. “QQ daohao heise chanyelian fanzui yanjiu” [The dark industry chain on stealing QQ account], *Gongan Lilun yu Shijian: Shanghai Gongan Gaodeng Zhuanke*

Xuexiao Xuebao 24, no. 4 (2014): 45-50.

Luo Bin. 2018. “Yidong zhifu xiqian fanzui yanjiu” [Research on the Crime of Money Laundering in Mobile Payment], *Xueshu tansuo* 8, (2018):102-106.

Ma Zhonghong. 2018. “Yi dianxin zhapian wei daibiao de xinxing wangluo fanzui zhencha nan dian ji duice yanjiu —Ji Yu W sheng de diaoyan qingkuang” [Challenges and countermeasures on telecommunication fraud: Based on the research in W Province], *Zhongguo Renmin Gongan daxue xuebao (shehui kexue ban)* 3:78-86.

McCarthy, N. 2018. “China now boasts more than 800 million internet users and 98% of them are mobile”, *Forbes*, 23 August 2018. https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/#70c20e1a7092

Meng Weide. 2019. *Kuaguo Fanzui* [Transnational Crime]. Taipei, Wunan.

Miniwatts Marketing Group. 2019. *Internet World Stats* Accessed 25 August 2019http://www.internetworldstats.com/stats.htm.

Shi Jihong. 2018. “A study on bitcoin-related crime and countermeasures”, *Journal of Information Technology and Society* 18: 64-79.

Shi Xiuxia. 2017. “Liyong xuni huobi xiqian fanzui yanjiu” [Research on money laundering using virtual money*]. Zhongguo Renmin Gongan Daxue Xuebao (shehui kexue ban)* 2: 32-41.

Song Peng. 2013. “‘Wangluo heishehui’: gainian , genyuan ji chengfang —Yi xingshi sifa wei shijiao” [Internet dark society: concept, origin and punishment—A lens from criminal justice*], Guizhou jingguan zhiye xueyuan xuebao* 3: 30-33.

Stanway, D. 2018. “China shuts thousands of websites in clean-up campaign: Xinhua”, *Reuters*, 23 September 2018. https://www.reuters.com/article/us-china-internet/china-shuts-thousands-of-websites-in-clean-up-campaign-xinhua-idUSKCN1M302F

Sun Bo and Du Zhenhua. 2017. “Lesuo ruanjian fazhan xianzhuang ji fang fan duice [Ransomware in spam: Current situation and countermeasures], *Tiaanjīn keji* 44, no. 3: 10-14.

Sun lijie and Zou Chen. 2016. “Hulianwang jinrong shidai daji kuajing xiqian de nandian yu tupo —E yizhong bianjing heihe shi weili" [Challenges towards combating cross-border money laundering in the age of internet finance- Take Heihe city as an example] . *Heilongjiang Jinrong* 12: 47-49.

Li, T. 2017. “QR code scams rise in China, putting e-payment security in spotlight”. *South China Morning Post*, 21 March 2017. Accessed 12 December 2019https://www.scmp.com/business/china-business/article/2080841/rise-qr-code-scams-china-puts-online-payment-security

Tie Yake, Dianxin wangluo zhapian de fazhi zonghe zhili —Yi hainan sheng danzhou shi zhili jngyan weili [Legal responses to telecommunication and internet fraud— Using Danzhou city in Hainan Province as an example], *Renmin Fazhi* 3: 68-74.

Trend Micro. 2016. *Cybercrime and the Deep Web*. Trend Micro (A Trend Labs Research Paper). Retrieved 12 December 2019. Accessed 12 December 2019. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cybercrime-and-the-deep-web.pdf

TWCERT. 2018. I*nformation Security Annual Report*. Taipei: Taiwan Computer Emergency Response Team.

Wang Huangyu. 2017. “The Interpretation and application of ‘aggravated false pretense”, *Essays on Criminal Police and Crime research* 20, (2017): 67-80.

Wang Gongzheng. 2017. “Yidong hulianwang biijing xia yidong zhifu xiqian fanzui ji qi fangkong” [Money laundering using mobile payment system and its prevention in the age of mobile internet], *Fanzui Yanjiu* 5: 55-64.

Wang Yalan. 2017. “Dianxin wangluo zhapian fanzui ji qi quzheng duice yanjiu.” *Fazhi yu Shehui* 1: 65-66.

Wong, Z. 2017."Exploring the Chinese Dark Web." Thesis in Criminology and Security, University of Liverpool.

Xu Peng. 2014. “Nadi yu gangao daji kuajing wangluo fanzui jingwu hezuo yanjiu” [Research on Police Cooperation among China Mainland, Hong Kong and Macau to Combat Cross-border Cybercrimes], *Fujian Jingcha Xueyuan Xuebao* 1: 65-73.

Yu, X., Su, M. and Li, Y. 2017. “Security Issues of In-Store Mobile Payment.” In *Handbook of Block chain, Digital Finance, and Inclusion volume 2*, edited by David Lee Kuo Chuen and Robert Deng 115-144. Academic Press

Yuan Lixīn, Gu Yijun and CiRen Luobu. 2018.“Hu lian wang hei se chan ye xian zhuang fen xi yu dui ce yen jiu” [Research and analysis on the Internet black industry], *Beijing Jingcha Xueyuan Xuebao* 6: 98-102.

Yeung, R. (2017). Mobile payment security gaps exposed at Hong Kong university. *South China Morning Post*, 28 September 2017. Accessed 12 December 2019, from https://www.scmp.com/news/hong-kong/law-crime/article/2113273/mobile-payment-security-gaps-exposed-hong-kong-university

Zhang Zheng. 2015. “P2P wangluo jiedai fanzui zhenfang yanjiu” [P2P internet loaning crime]. *Anhui Jingguan Zhiye Zueyuan Xuebbao* 6: 44-47.

Zhu yunxi, Wangluo xiqian fanzui de zairenshi. 2018. “Cong hulianwang xinxingshi jiaodu fenxi” [Re-recognition of the network crime of money laundering], *Hunan Jingcha Xueyuan Xuebao* 4: 68-73.

Section IV: Lessons from the Hispanophone Literature

Introduction

The phenomenon of globalization, along with the widespread use of the computer and technological developments, have contributed to the growth of cybercrime in the world, while increasing the criminal indicators of theft. Behaviours, such as theft by electronic means, affect both individuals and institutions. In addition, the emergence of new virtual currencies has raised questions about their security and transparency in the money market, given the existence of scarce legal regulation, regarding investment with virtual currencies.

Private and public bodies have responded to increased cyberattacks by putting in place technological countermeasures to fight cybercrime, such as forensic digital analysis and software tools. However, the measures undertaken by nations to control cyberspace and combat cybercrime are still meagre and dissimilar among many regions in the world.

The cybercrime literature written in Spanish for Hispanophone audiences has grown exponentially in response to emerging and evolving threats facilitated by the digital environment. A subset of the literature has focused on the financial dimensions of narcotrafficking and money-laundering from a cybercrime perspective. Although there is significant research in the Spanish-speaking community that acknowledges the impact of cybercrime at different levels (i.e., individual, corporate, and institutional), only a few studies have examined how offenders profit from their crimes, identified important gaps in legislation around transactional cybercrime, or studied the responses of governments to these criminal activities.

This section presents a systematic review of the knowledge offered in the Spanish transactional cybercrime literature in four major, Spanish-speaking countries with a high population of Internet users: Argentina, Colombia, Mexico, and Spain. The first part of this section discusses the methodology used to conduct the review and locate relevant articles. The second part of the section provides an overview of the national cybersecurity strategies used by each of the countries to counter cybercrime, including financial crimes. The third part discusses the lessons learned from this review, highlighting what we know about cybercriminal ecosystems, the effectiveness of private and public sector initiatives to respond and disrupt these ecosystems, and norms and regulations established by these countries to judicialize transactional cybercrime. Finally, the report comments on the limitations found in the Hispanophone literature pertaining to criminal financial transactions in cyberspace.

Methods

This report focuses on Spanish-language sources. It consists of a systematic review of the literature on criminal transactional methods in four countries with a high population of internet users: Spain, Argentina, Colombia, and Mexico. The objective of the review is to summarise criminal transaction methods as described by Hispanophone researchers. This review examined a variety of academic, scientific, and government documents. In specific, this report drew its results from various academic and non-academic sources, including conceptual essays, policy analyses, white papers, and empirical analyses. In addition, it studied books and book chapters, scientific articles, and government and think-tank reports. Consistent with the English review, it retrieved only articles published from 2013 to June of 2019 that are publicly accessible or accessible through university databases.

To capture a wide range of literature that examines illicit transactional methods in cybercrime, we adopted a five-step process. First, a keyword search was conducted, using *Dialnet* citation database, which is the largest database of scientific articles in Spanish. *Dialnet*'s consolidation is the result of a public and open project led by the University of La Rioja with a high participation of libraries, journals, and universities in Spain, but also from other parts of the world. This cooperation has led to the portal's success. In addition, we searched the Spanish Google Scholar indexing database. Google Scholar covers academic work and documents outside the academic scope that may have an important impact on issues of transactional cyberspace and that may not be captured in standard academic citation index databases. Where applicable, similar keywords to the English review with their corresponding translations were used to limit the searches:

Main word Secondary word

I.e., Cybercrime + i. Money

> ii. Theft
>
> iii. Corruption
>
> iv. Extortion
>
> v. Cryptocurrencies

In other cases, we searched for specific words and phrases that are not direct translations, but phrases employed commonly in the Spanish language that make sense to Spanish speakers. For example, the Hispanicisation of cybercrime, ‘cibercrimen’, is often used to define an illicit activity delivered through electronic means. However, the expression ‘delincuencia informática’ (ICT delinquency) better defines cybercrime as a general concept in Spanish. There are other terms that have broad cultural meaning for financial issues of transactional cyberspace in Latin America which were used in this analysis:

In Spanish Translation

i. Estafa informática Computer scam

ii. Delito informático Computer crime

iii. Delincuencia informática Cybercrime

iv. Ciberpiratería Cyberpiracy

v. Derecho penal informático Computer criminal law

Second, the research team searched relevant Hispanophone cybercrime and criminology journals, using the same search terms as above. Literature in Spanish on financial issues of transactional cyberspace was found in relevant journals that cover diverse fields of study, including cybercrime, criminology, intelligence, security studies, cyber-security, and data security/protection. The Spanish journals surveyed included

La Revista Española de Investigación Criminológica (REIC), *La Sociedad Española de Criminología y Ciencias Forenses* (SECCIF), and *La Revista de Estudios en Seguridad Internacional* (RESI). The key Argentine journals surveyed included *Revista de Derecho Penal y Criminología* (RDPyC), *Revista Pensamiento Penal* and *Revista de Derecho Penal y Criminología*. The Colombian journals consulted included *Asociación Colombiana de Criminología* (ACC), *La Revista Criminalidad* (Rev. Crim.) *National Police and Revista Científica General José María Córdova*. And the Mexican journals reviewed were *Archivos de Criminología, Seguridad Privada y Criminalística*; and, *Crimen transnacional organizado y seguridad internacional: cambio y continuidad, and Criminogénesis*.

Third, this review included targeted searches among university journals in the nominated Spanish-speaking countries. Literature in Spanish that deals with malware issues fall within the academic interests of recognised university journals. These include, in Spain, the *Revista de l'Institut Universitari d'Investigació en Criminologia* (University of Valencia), *Crítica Penal y Poder* (University of Barcelona), and *La Revista de Derecho Penal y Criminología de la UNED* (National Distance Education University – Madrid); in Argentina, *the Revista Argentina de Derecho Penal y Procesal Penal* (Austral University), *Instituto de Relaciones Internacionales* (La Plata National University), and *Revista de Ciencia Política y Relaciones Internacionales de la UP* (University of Palermo); in Colombia, *La revista de Derecho Penal y Criminología* (Externado University of Colombia), *Papel Político* (Pontifical Xavierian University), and *Colombia Internacional* (University of the Andes); and, in Mexico, *the Revista de Investigación en Derecho, Criminología y Consultoría Jurídica* (University Autonoma of Puebla), *Criminología y Sociedad* (University of Sciences of Nuevo León) and *Visión criminológica-criminalística Colegio Libre de Estudios Universitarios* (CLEU).

Fourth, the research team conducted a targeted search among government agencies, think tanks, and non-profit organisations in the Spanish-speaking nominated countries. Most of these countries possess a well-defined national cyber security strategy; as a result, important information on financial issues of transactional cyberspace was gathered from government sites. Additional agencies, including non-profit organisations that fall within the scope of crimeware in those countries, have been searched. These include the following: In Spain, the El Ministerio del Interior (Ministry of the Interior), and the Centro de Ciberseguridad Industrial (Industrial Cybersecurity Center); in Argentina, the Ciencias Penales desde el Sur (Criminal Sciences from the South); in Colombia, Asobancaria and Informática Forense Colombia (Colombia National Forensic), and, in Mexico, Comexi.

The search yielded a high number of articles, books, book chapters, reports, and white papers. For our analysis, we retained a total of 81documents: 25 documents for Argentina, 21 for Colombia, 18 for Mexico, and 27 for Spain. The studies selected used empirical data or were conceptual pieces that provided novel insights into the financial infrastructure of cybercrime.

The State of Play in Hispanophone Regions of Focus: Law Enforcement Bodies, Socio-political Considerations, and Known Trends

This section provides an overview of the relevant cybercrime strategies and regulations, the bodies in charge of responding to cybercrime and financial crime in Argentina, Colombia, Mexico, and Spain. These countries all possess a coherent national cybersecurity strategy with clear objectives and policies. However, most countries in Latin America lack *both* a clear national cybersecurity strategy and the capacity to respond to cyberattacks. Apart from the countries studied here, only Panamá, Paraguay, Chile, and Costa Rica possess a cybercrime national policy. Contributing factors to the slow adoption of cybercrime policies in the Latin American region include the lack of resources dedicated to this issue and the lack of practical experience and specialised knowledge to design and implement this type of measures (Hernández 2018).

Argentina

National Cybersecurity Strategy

The Estrategia Nacional de Ciberseguridad de La República Argentina (2019)(National Cybercrime Strategy of the Argentine Republic)established a set of basic principles to allow for the protection of cyberspace, so that it may be safely used and accessed by individuals and public and private organizations. The strategy, established by the Argentinian national executive branch in charge of the Cyber Security Committee[69], decreed concrete actions against cyber threats through eight fundamental objectives:

- Awareness of the safe use of cyberspace. The strategy includes society as a whole, embracing the private and public sectors and civil society organisations, to promote an educational awareness of the risks that cyberspace poses and to create a culture of good habits in the use of cyberspace.
- Training and education in the safe use of cyberspace. The process involves the acquisition of knowledge, skills, and abilities for the safe use of cyberspace. It requires the training of professionals, technicians, and researchers. The execution of

such educational activities must include workshops and trainings in the academic, governmental, and private sectors.

- Development of the regulatory framework. It is imperative to generate legal norms, regulatory frameworks, and protocols to address the challenges posed by the risks of cyberspace. To that end, the Argentinian legal framework must consider the common principles, technical standards, and good practices that are set and recognised by the international community.
- Strengthening prevention, detection, and response capabilities. The Argentinian security agencies, in cooperation with the investigation and prosecution of crime, organised crime, and terrorism in cyberspace, must strengthen their prevention, detection, and response capabilities against the use of cyberspace for illegal purposes. Better analysis capabilities at different yet co-ordinated levels (provincial, local, and national) will ensure a more effective protection of national interests.
- Protection and recovery of public sector information systems. The strategy aims to develop public policies oriented to protect the public sector information systems. The information security polices of Argentina must work in a coordinated and decentralised manner whereby agencies of the national public administration, provincial administrations, and the administration of the autonomous city of Buenos Aires cooperate with one another. The implementation of these policies includes the application of the information security policies that allow for the recovery and resilience of public sector information systems.
- Promotion of the cybersecurity industry. The goal is to promote the continuous development of the national industry in all sectors linked to cybersecurity. It is important to provide industries with the technological capabilities necessary to combat various cyber-threats, while promoting research, development, and innovation activities, both in the public and private sectors.
- International cooperation. The national cybersecurity strategy looks to improve its participation in cybersecurity affairs in the international arena. It will develop regional and international agreements that contribute to the generation of a peaceful and safe cyberspace. It also aims to strengthen the presence of Argentina in all international organizations, including academic and technical fields, in terms of cybersecurity.
- Protection of national critical information infrastructures. With this final objective, the strategy aims to strengthen the public-private cooperation in safeguarding critical information infrastructures in the country. Hence, coordinated efforts within industrial networks allow for the development of detection, protection, and response

capabilities in the face of threats, while safeguarding critical and productive digital services.

Financial and Cryptocurrency Regulation

According to Humar (2008), Argentina effectively has two institutions responsible for supervising its financial system: The Central Bank and the Superintendence of Financial and Exchange Entities. The Superintendence of Financial and Exchange Entities operates under the Central Bank, which exercises supervisory functions of financial and exchange activities through the Superintendence. These two administrative bodies rule all the financial activity in Argentina in light of Law 24,144 of 1992, Organic Letter of the Central Bank. This legislation includes several responsibilities and objectives to advance adequate banking supervision.

Accordingly, the Central Bank of the Argentinian Republic, through the Superintendency, regulates the financial sector and the individuals and organisations that supply or demand of financial resources in Argentina. Within the framework of the law, commercial banks, investment banks, mortgage banks, savings and loan companies for housing and other real estate, and credit cooperatives are subject to its mandates (Humar 2008).

Senator Silvia Elías de Pérez, president of the National Economy Commission of the Senate, notes that cryptocurrencies lack a regulatory framework in Argentina, even though they are becoming increasingly important in the financial market. The senator further notes that Argentinians need to transition into this type of currency in a safe manner, while avoiding complex risks, such as money laundering fraud (El Economista 2019b).

As a result, Argentina is considering the regulation of cryptocurrencies, thus guaranteeing greater security for investors and negotiators who operate with digital currencies. Entities such as the Central Bank of Argentina, the National Securities Commission of Argentina, and the Financial Training Unit of Argentina are interested in achieving a regulation that is consistent with the needs of the country's economy. Despite its participation at the Financial Innovation Table, the Central Bank of Argentina, at least for the moment, has limited itself to observing the evolution of virtual currencies and their associated technologies (Criptodinero 2019).

Colombia

National Cybersecurity Strategy

Colombia’s *Agenda Estratégica De Innovación: Ciberseguridad* (Strategic Innovation Strategy for cybersecurity) (MinTIC 2014) seeks to generate national cybersecurity policy guidelines aimed at developing a national strategy that counteracts the increase in computer threats that affect the country. The government defines cybersecurity as the capacity of the state to minimise the level of risk its citizens face through threats of a cybernetic nature.

The strategy has been framed around strategic vectors that the government has identified as priorities for Colombia, while strengthening the country's position in terms of cybersecurity. Each of these vectors is composed of thematic lines, which detail the specific topics on which innovation efforts in the country should be focused. For example, Colombia has made great progress in terms of policies, procedures, controls, and technical recommendations for strengthening state cybersecurity. In turn, these developments have closed the existing gaps, in terms of prevention, control, and reaction policies in the face of the constant increase in computer threats.

The innovations in this development vector are framed under the following thematic lines:

- Generation of policies, norms, and other legal forms to dictate the technological and procedural guidelines of exchange of information among different state entities, between government and industry, and among the general public, under schemes that guarantee the integrity, confidentiality, and availability of information;
- Generation of policies, norms, and other legal forms aimed at strengthening the capacities and organization of the Colombian state to protect cyberspace from threats that affect national sovereignty and constitutional principles;
- Incorporation of cybercrime as a fundamental element of policies, norms, and administrative acts, which will provide the state the capacity to identify, recognise, and adequately judge cybercrime issues in legal and constitutional processes;
- Generation of guidelines for the protection of the confidentiality, integrity, and availability of data relevant to the Colombian state through the definition, adoption, adjustment, update, incorporation, implementation, and evaluation of technological schemes and procedures;
- Incorporation of software in state entities according to national information security and cybersecurity policies;

- Generation of policies, norms, and other legal forms aimed at strengthening alliances and international cooperation to combat threats and crimes of a cyber nature; and
- Generation of policies, norms, and other legal forms to strengthen the capacities of the state to guarantee adequate identification of Colombian citizens, provide authorizations, as well as the protection of their identity.

One of the fundamental goals is of Colombia’s cybersecurity strategy to ensure adequate knowledge and development opportunities for public officials and society in general on issues related to cybersecurity. Given this new complexity, it becomes imperative for the Colombian government to establish innovation projects that include quality education and training to human resources. These include:

- Establishment of programs of technical, technological, and professional training of high level and international quality that consider legal issues of information security and cybersecurity;
- Definition, adoption, structuring, implementation of pedagogical and educational practices in information security for all state entities, along with teaching models and incorporation of knowledge, skills, and abilities in information security and cybersecurity;
- Analysis, design, structuring, implementation, and evaluation of awareness and appropriation strategies aimed at the community in general, by political, socio-economic, cultural, and educational sectors;
- Response to modern challenges, taking into account the associated technological complexity and the wide variety of entities that make up the Colombian state;
- Structure, design, development, and implementation of models for the measurement of maps of risks, threats, and vulnerabilities, existing in the government's information systems and for individual entities that allow comparable measurement by groups of entities (for example, productive sectors). This will facilitate decision-making, regarding prevention, protection, and early detection of incidents;
- Structure, design, and implementation of models for incident management, that will allow responding, alerting early, and properly dealing with incidents of a cybernetic nature;
- Structure, design, and implement of models for the use of critical assets and technological resources of the Colombian state, as well as for the incorporation of new resources in order to minimise risks associated with the transport, processing, and storage of critical information;
- Structure technological and methodological schemes of simulation of cyberattacks that allow for the early identification of the risks of a cyber nature to which the

Colombian state is exposed, and that provide the state with preventive and reactive capacity;

- Define, adopt, structure, create, and implement incident response centres at various levels (national, regional, and local), in line with initiatives and efforts raised by the ColCERT (Colombian Cyber Emergency Response Group) and the CSIRT (Computer Security Incident Response Services) of Colombia.

Financial and Cryptocurrency Regulation

The Superintendencia Financiera de Colombia (SFC) Financial Superintendence of Colombia is a technical body attached to the Ministry of Finance and Public Credit, with legal status, and administrative and financial autonomy. The SFC supervises the Colombian financial system in order to preserve its stability, security, and confidence, as well as to promote, organise, and develop the Colombian stock market and the protection of investors, savers, and insurance agents (Superintendenca Financiera de Colombia 2019). The President of Colombia, in accordance with the law, exercises, through the SFC, the inspection, surveillance, and control of individuals and organisations which carry out financial, stock market, insurance, and other activities related to management, exploitation, or investment of financial resources.

The SFC pronounced, through Circular Letter 29 of 2014, that virtual currencies are neither regulated by law nor subject to the control, surveillance, or inspection of the Superintendency, thereby establishing the risks and non-existence of virtual financial mechanisms to force compliance with cyber transactions. In addition, entities monitored by the SFC are prohibited from guarding, investing in, or transacting with digital currencies (Externado University 2019).

Colombia has taken its first steps towards cryptocurrency regulation. Colombia aims to regulate how individuals and institutions use crypto-assets through its Unique Registry of Crypto Exchange Platforms (RUPIC). On April 4, 2019, a draft regulation (which has yet to be enacted at time of writing) was published with specifications designed to regulate the Crypto Exchange Platforms (PIC). The Colombian government has asked the cryptocurrency community to respond to the draft, thus seeking to integrate the voice of the people in the creation of the law. Also, the Colombian authorities wish to avoid the risks that cryptocurrencies entail. As a result, the draft recommends that institutions implement preventive measures against money laundering and terrorist financing through virtual currencies, such as Bitcoin (Colombia Fintech 2019).

Mexico

National Cybersecurity Strategy

The *National Cybersecurity Strategy* (*Estrategia de Ciberseguridad Nacional*, ENCS) (Government of Mexico 2017) defines objectives, presents guiding principles, identifies the different actors involved, and clarifies the efforts created by individuals, civil society, and private and public organizations in cybersecurity. It also explains the governance approach for the implementation, monitoring, and evaluation of the strategy.

General objective:

The objective of the strategy is to strengthen cybersecurity actions applicable to the social, economic, and political spheres that allow individuals and public and private organizations to use ICT (Information and Communications Technology) in a responsible manner, along with a sustainable development of the Mexican state. The Strategy includes the following as guiding principles:

- Human rights: Contemplates the promotion, respect, and fulfillment of human rights in different cybersecurity actions. These rights also include freedom of expression, access to information, respect for privacy, protection of personal data, and health, education, and work rights.
- Risk management: Handles uncertainty scenarios through preventive and corrective approaches, with the intention of minimizing the impact of the changing threats and risks of cyberspace.
- Multidisciplinary and multi-stakeholder collaboration: Supports a multidisciplinary collaboration of different parties (actors and sectors) of the Mexican community, allowing for a holistic development of the strategy while promoting open and transparent participation.

The National Cybersecurity Strategy is the official document that reflects the general actions to be carried out by the Mexican state as a whole, including civil society, academia, private sector, and public institutions, so that the maximum benefits of ICT are obtained in a reliable and resilient environment that is beneficial for all. To achieve the general objective, the strategy raises five strategic objectives, the development of which requires eight transversal axes. All of the actions of each transversal axis were developed upon the three main guiding principles delineated above.

Strategic objectives:

- Society and rights: Generate appropriate conditions for the population to carry out their activities in a responsible, free, and reliable way in cyberspace. This will improve their quality of life in a framework of respect for human rights, which include freedom of expression, privacy, and personal data protection.
- Economy and innovation: Strengthen cybersecurity mechanisms to protect the economy and the different productive sectors of the country while promoting technological development and innovation. In addition, efforts will be concentrated to boost the national cybersecurity industry, to contribute to the economic development of individuals, organizations, private and public institutions, and society in general.
- Public institutions: Protect the information and computer systems of public institutions in the country to promote optimal functioning and continuity in the provision of services and procedures to the general community.
- Public security: Increase capacities for the prevention and investigation of criminal behaviour in cyberspace that affect people and their heritage, in order to maintain order and public peace.
- National security: Develop capacities to prevent risks and threats in cyberspace that can alter national independence, integrity, and sovereignty, and that can affect development and national interests.

Transversal axes:

- Cybersecurity status: Create a set of values, principles, and actions that take place in the form of education and training, carried out by society, academia, the private sector, and public institutions, so that these actors can interact in cyberspace harmoniously, reliably, and as a factor of sustainable development.
- Capacity development: Undertake a set of actions aimed at generating and strengthening the organizational capabilities, human capital, and technological resources in cybersecurity, so that society, academia, the private sector, and public institutions can obtain the resources needed for risk management and threats in cyberspace, as well as for increasing national resilience.
- Coordination and collaboration: Develop a set of actions aimed at coordinating and establishing the collaboration channels among the different agents, such as public institutions, academia, civil society, and private organizations in cybersecurity, with the purpose of consolidating the cybersecurity ecosystem of Mexico. In doing so, the state will obtain the resilient capacity necessary to establish the preventive, proactive, and reactive mechanisms necessary to provide confidence and tranquillity to the population in their use of ICT.

- Research, development, and innovation in ICT: Establish a set of actions aimed at establishing mechanisms to promote research, development, and innovation in the use and exploitation of cybersecurity technologies that promote the development of human capital and technological innovation in the field of national cybersecurity.
- Standards and technical criteria: Create a set of actions focused on the development, adoption, and strengthening of technical and technological standards in cybersecurity, which allow the application of best practices and processes in the use of ICT around the cybersecurity environment.
- Critical infrastructure: Develop a set of actions aimed at establishing the necessary mechanisms to minimise the likelihood of risks and vulnerabilities in the use and management of ICT, as well as strengthening capacity to maintain the stability and continuity of services in case of a cybersecurity incident.
- Legal framework and self-regulation: Promote and establish actions and mechanisms necessary for the adaptation of a national legal framework linked to cybersecurity and for self-regulation by concessionaires, permit holders, and distributors of ICT services, so that internet intermediaries and society, in general, can use ICT and enjoy a healthy coexistence in cyberspace.
- Measuring and following up: Create a set of policies and actions aimed at the promotion and development of measurement mechanisms that allow the monitoring of results obtained from the implementation of the National Cybersecurity Strategy and its impact on the social and economic development of the country. The policies will also identify areas of opportunity for continuous improvement.

Financial and Cryptocurrency Regulation

The National Banking and Securities Commission (CNBV) is a decentralised body of the Ministry of Finance and Public Credit. It has the power to authorise, regulate, supervise, and sanction the various sectors and entities that make up the financial system in Mexico, as well as those individuals and corporations that carry out activities related to the financial system. Its goal is to ensure its stability and proper functioning, as well as to maintain and promote the healthy and balanced development of the financial system as a whole, while protecting the public interest. The vision of the CNBV is to be an efficient, modern, and respected authority that seeks the stability of the financial system in Mexico, in accordance with best international practices, and that contributes to the construction of a prosperous Mexico, where each family has access to more and better financial services (Comisión Nacional Bancaria y de Valores - Government of Mexico 2019).

According to Pérez (2019), Fintech, the first crypto-regulation enacted in Mexico, began to apply to crypto companies in September 2019. At present, Mexico is the third country in Latin America (after Colombia and Brazil) with the highest use of digital assets. Mexico is the leader in Latin America, in creating a specific law for the regulation of companies in the financial technology sector. Currently, three entities in the country are in charge of regulating the cryptocurrency sector: Bank of Mexico, Ministry of Finance and Public Credit, and the National Banking and Securities Commission (CNBV).

However, despite being a world leader in terms of adopting crypto regulation, Mexico still offers much uncertainty as to the scope of its legal framework. Technological consultant Eloísa Cadenas suggests that one of the most outstanding features of the new regulation is that it recognises cryptocurrencies as digital assets, which, in other words, are electronic payment mechanisms (El Economista 2019a). Thus, the institutions responsible for regulating cryptocurrencies in Mexico such as the Bank of Mexico should consider the volume of transactions, the relationship between crypto assets and exchange houses (exchanges) that exist in Mexico, the liquidity of each cryptocurrency and the traceability that can be done on each asset and the cryptocurrency’s vulnerabilities (El Economista 2019a).

According to the regulatory framework for digital assets, the Bank of Mexico had to determine by March 2019 which cryptocurrencies it would authorise for commercial use in the country. However, when the date arrived, the agency did not authorise any cryptocurrencies; instead, it recommended that investors distance themselves from acquiring assets of this type (Pérez 2019).

Spain

National Cybersecurity Strategy

The National Cybersecurity Strategy (*Estrategia de Ciberseguridad Nacional*) by the Presidencia de Gobierno (2013) designed and adopted in 2013 Spain’s cybersecurity plan, which formulates strategies around twelve areas of action. This strategic document supports the collective capacities of a nation that is firmly committed to ensuring its security in cyberspace. From the perspective of the presidency of the government, advances in the field of cybersecurity also improve Spain’s economic potential, as they promote a safer environment for investment, job creation, and competitiveness.

The National Cybersecurity Strategy is the reference framework of an integrated model based on the involvement, coordination, and harmonization of all state actors and resources, including public-private collaboration and citizen participation. Also, given the transnational nature of cybersecurity, cooperation with the European Union and international regional bodies with competences in the field are an essential part of this model. To achieve its objectives, the strategy creates an organic structure that is integrated into the framework of the National Security System. This structure serves to articulate the unique action of the state in cybersecurity affairs.

The Strategy consists of five chapters. The first chapter presents the characteristics that define cyberspace and the opportunities cyberspace offers from the point of view of security. It notes how society is becoming more dependent on Information and Telecommunications Systems (ICT) and cyberspace day by day. As a result, knowing the threats, managing risks, and articulating an adequate capacity for prevention, defence, detection, analysis, investigation, recovery, and response are essential elements of the National Cybersecurity Policy.

The second chapter establishes the purpose and guiding principles of cybersecurity. The Strategy has set directives for the safe use of cyberspace, promoting an integrative vision, which will help to guarantee the nation’s security and progress, in coordination and cooperation with the public and private sectors and citizens. These directives fall within the principles set forth in the constitution, within the provisions of cyber affairs of the United Nations, and within initiatives developed in the European, international, and regional frameworks.

In the third chapter, the strategy addresses the cybersecurity objectives. The global objective is to ensure that Spain makes safe use of ICT, strengthening the capacities for prevention, defence, detection, analysis, response, and recovery to cyber-attacks. In addition, the National Cyber Security Policy must serve the following purposes:

- For public administrations: ensure that all ICT used by them has the appropriate level of security and resilience;
- For companies and critical infrastructure: promote the security and resilience of networks and information systems used by the business sector and operators of critical infrastructure;
- For the judicial and policing fields: strengthen prevention, detection, response, investigation, and coordination capacities against activities of terrorism and crime in cyberspace;

- Among citizens, professionals, companies, and the public administration: raise awareness of risks arising from cyberspace;
- For various sectors of the community: provide training and the skills, experience, and technological capabilities that Spain needs to achieve all its cybersecurity objectives; and,
- In terms of international collaboration: contribute to the improvement of cybersecurity, supporting the development of a coordinated cybersecurity policy with the European Union and international organizations.

The fourth chapter includes the Lines of Action of National Cybersecurity. Hence, the Government of Spain, recognizing the importance of building and maintaining trust in ICT used by citizens, professionals, companies, and public sector organizations, will promote information and awareness campaigns necessary to ensure that everyone in the community is aware of the risks of operating in cyberspace and has access to the tools that enable their protection.

The final chapter establishes the organic structure of the service of cybersecurity. Under the direction of the President of the Government, the structure is made up of three organs: the National Security Council, acting as the delegated commission of the Government for National Security, and two new ones: the Specialized Cybersecurity Committee, which will support the National Security Council by assisting in the direction of the National Security Policy in cybersecurity, while promoting collaboration between the public administration and the private sector, and the Specialized Situation Committee, which will manage crisis situations of cybersecurity that, due to their nature or dimension, could exceed the response capabilities of the regular mechanisms.

Financial and Cryptocurrency Regulation

According to Credimarket (2013), there are several institutions in Spain that exercise control and inspection functions and are of a regulatory and sanctioning nature:

- *Bank of Spain* is the national central bank and the supervisor of the Spanish banking system. Since January 1, 1999, the Bank of Spain has been entrusted with various functions, such as the implementation of the monetary policy of the euro zone, the performance of foreign exchange operations, and the management of the official foreign exchange reserves of Spain.
- *European Central Bank* is the central bank of the European Union, responsible for managing the monetary policy of the 17 member states of the euro area. It was

established by the Treaty of Amsterdam in 1998 and is based in Frankfurt (Germany). Among the main objectives of the ECB are maintaining price stability in the euro region, defining and executing the monetary policy of the euro zone, performing foreign exchange transactions, and managing the official foreign exchange reserves of the member countries of the euro zone.

- *National Securities Market Commission* (CNMV) is the body responsible for the supervision and inspection of the Spanish stock markets and the activity of those involved in it. Its main objective is to ensure the transparency of the securities markets, the correct formation of prices, and the protection of investments.
- *General Directorate of Insurance and Pension Fund of the Ministry of Economy* is responsible for monitoring compliance with the requirements for access and expansion of private insurances. It also exercises financial supervision of the insurers of pension funds in Spain.

Spain has no clear regulations regarding cryptocurrencies. Bitcoin and other cryptocurrencies are not considered money, since they are not issued by the Spanish government; however, crypto assets can be considered as digital products (Territorio Bitcoin 2019). The president of the National Securities Market Commission (CNMV), Sebastián Albella, believes that cryptocurrencies, which do not act as ‘mere deposits,’ must be subject to the same rights as negotiable securities; thus, cryptocurrencies have claimed competences in this sense. Albella has recognised that there are ‘certain mismatches’ in the regulations because cryptocurrencies are a new phenomenon, and Spain is working at the European level to address the issue in a ‘coordinated’ way (ABC 2018).

Review of the Transactional Spanish Cybercrime Literature

The Ecosystem of Cybercrime

For scholars, such as Saín (2018), computer crimes can be classified into two large groups: those that require technical sophistication for their execution, usually through malicious programs developed by hackers that seek to violate devices or networks and those that require ‘social engineering’, which deceive users by the use of threats, fraud, and grooming. In general, computer crimes are undertaken for an economic purpose and seek to take money from their victims, or the crimes produce what is called identity theft, by obtaining personal or institutional data from third parties.

Other scholars, such as Martínez (2018), classify unlawful computer-facilitated behaviours and cybercrimes, according to the different types of victims impacted:

- Violations committed through social networks such as attacks on intimacy, honour, and moral integrity,
- Stalking and malicious persecution or harassment against a person that can be carried out through the internet or other electronic means,
- Child sexual exploitation and the development of child sexual exploitation materials,
- ‘Cyberhate’ activities, which include xenophobia, racism, and discrimination,
- Crimes against intellectual property, and
- Scams and frauds, including behaviours that undermine the economic patrimony of third persons.

In terms of transactional cybercrime, various illicit activities have been recognised by the Hispanophone literature in the recent years. New technologies have contributed to this “economic, social, and political” development. Cryptocurrencies, for example, have become an important international financial tool, while other types of crime, such as scams, have increased at the same rate as their expansion (Revista Pensamiento Penal 2018). However, at the same time that technological advances facilitate economic development, they also increase the possibility of individuals’ committing harmful and dangerous behaviours against third parties. Lucrative computer crimes, in many cases, transcend borders, reaching an effective global progression.

Cybercriminals constantly see opportunities to make a profit by different cybernetical means, with attacks that generate income without a relative amount of effort. Technological developments contribute to the growth of cybercrime; current threats that are attacking cyberspace generate multimillion-dollar losses (Martínez Moya 2016). The literature that studied cybercrime in Hispanic countries is aware of the negative impact and the great economic cost that individuals and organisations pay due to cybercrime attacks. According to Reyes Neira (2015), at the global level, approximately one in five organizations that suffered from financial crimes have experienced a financial impact of between USD $1 million and $100 million[70]. And the percentage of entrepreneurs who reported losses of more than USD $100 million doubled, from one to two percent over the course of three years. For example, in 2015, in Colombia alone, 7,118 cyber-attacks were recorded, which was an increase of 40% over 2014. The economic losses derived from these acts represented in 2014 around 0.14% of the National GDP, that is, approximately USD 500 million.

The Spanish literature on transactional cybercrime notes that, in the social sphere, adolescents play a critical role in criminal online activities since they are part of a generation that has been immersed in, and have faculty with, the world of digital technology. Hence, they are more exposed to risks and dangers online: violation of privacy, theft or impersonation, emotional abuse, sexual abuse, such as grooming, exposure to inappropriate or misleading material, cyberbullying, and phishing Diaz and Pinto (2014). At the same time, young people with low ethical standards are more likely to explore cyberspace in search of economic income and recognition among their peers. Roibón (2019) notes that the cybercrime industry which recruits young people is diverse. Some of the recruits, given their inexperience, begin by making attacks that require little complexity or sophistication. Others work for organisations comparable to those of a software company that has its employees perform processes of marketing and distribution of technological applications and other malicious software.

Main Transactional Cybercriminal Activities in the Hispanophone Literature

Illicit Use of Cryptocurrencies

Pérez López (2017) describes the illicit uses of cryptocurrencies in Spain, which conform to the classic characteristics of cybercrime. Given the materialised and cross-border nature of cybercrime, it is not surprising that in the use of cryptocurrencies in the context of financial crime, Spanish authorities profile crimes very similar to those found in other European countries. Typically, cryptocurrency scammers collect funds by convincing their victims to participate in a cryptocurrency investment fund or in an initial cryptocurrency offer. Such investments often follow a Ponzi or pyramid scheme so that the criminals can receive a constant flow of money over a certain period of time. Between 2013 and 2015, cryptocurrency scammers collected money from an estimated 50,000 victims throughout the world, by promising them very high returns on investment. The returns were to be accrued in a non-existent cryptocurrency, created by the organisers of the scam.

Pérez López (2017) further describes that the criminals combined several means of laundering the benefits obtained, which varied depending on their country of origin. Through ransomware, they obtained in Europe prepaid codes from Ukash or PaySafeCard (British and Austrian providers, respectively, of electronic money), and, in the US, from MoneyPak (American provider of Visa credit cards and prepaid MasterCards), acquired by the victims themselves. Many of the codes were sold in Russian forums, and the product of the sale was either entered into online payment services through the use of false or stolen documentation, laundered through online casinos, or converted into cryptocurrencies (in particular, Bitcoins). Some of the American Moneypak cards were obtained in the US, sent by parcel post, and activated in Spain. Later, the money was withdrawn in ATMs by a network of ‘mules’ dedicated to that activity. To hinder its traceability, the cash could then be reintroduced into the electronic money circuit to continue being converted into different means of payment. A large part of the organization's benefits ended its conversion cycle in Bitcoins.

Social Engineering Scams

Social engineering is a fraudulent technique of obtaining confidential information, access to or privileges in information systems, through the manipulation of legitimate users. Social engineering is based on the idea that users are the weakest link in the security chain; thus, it takes advantage of the natural tendency of people to trust and react predictably to certain situations. Criminals take advantage of vulnerabilities and emotions, such as fear, compassion, happiness, euphoria, and any other feelings that are capable of generating reactions that end up violating the victim's security. After victims are psychologically manipulated, they share confidential information about themselves or their organizations. Most of the time, attacks are carried out by email or telephone. As it is a more human issue, the technological tools that companies implement cannot prevent effectively these types of attacks.

According to Meseguer González (2013) online frauds also proliferate among internet users, such as online shoppers, job seekers, and romance seekers. In the job seeker fraud, victims receive an email from an unknown sender that offers a job offer, promising a great salary; however, the goal is to get the victims to make bank transfers. In addition, there has been a significant increase in the number of scams with fake antivirus programs that trick victims into making online purchases so that the scammers can obtain the victims' bank data.

Other fraudulent modus operandi are achieved through online dating sites. Online fraudulent dating plays with the emotions of its victims. The typical online dating scam begins when the scammer posts an attractive photo on an online dating site. The scammer then sends messages to other members of the website expressing interest. The next step uses the Nigerian fraud technique, also known as 'advance payment fraud'. Here, the contacting person poses as a foreigner who, in addition to dating, needs help withdrawing millions of dollars from the country and offers the recipient a percentage of his fortune for helping him with the transfer. Many of the victims have lost several thousand dollars in the process because cybercriminals request several payments in advance to facilitate the deal (Meseguer González 2013).

Phishing

Phishing is a model of computer abuse considered to be a type of social engineering which involves acquiring confidential information fraudulently (such as, a password or detailed information about credit cards or other bank information). The cybercriminal pretends to be a trusted person or agent in charge of an official communication made by instant messaging systems or even via phone calls.

Reygadas (2018) defines phishing activities as expropriations designed to dispossess through the illegal and unauthorised appropriation of information and other digital resources in order to carry out a robbery, fraud, or similar criminal activity. Criminal groups appropriate data and passwords of people or companies to obtain an economic advantage, for example, to make purchases with the credit cards or subtract funds from bank accounts. These types of fraudulent activities, carried out by criminal groups, involve an unauthorised appropriation of information that is then used in a second illegal criminal activity, such as fraud or theft.

Phishers or scammers can also pretend to belong to banking entities and ask cyber-navigators for their credit card credentials, through a form usually linked to a false website that presents an appearance similar to the original. Once they manage to deceive the recipient of the message, they obtain access to the victim's account and make transfers or withdrawals of monies from the account. Through usurpation or impersonation activities, criminals use personal data to impersonate the individual whose identity has been stolen. These robberies, in combination with the anonymity of online transactions and other activities, are used to commit a series of crimes, including fraud, terrorist activities, bank fraud, online extortion, money laundering, and smuggling.

A common phishing activity involves the mass sending of emails that appear to come from reliable sources to a company or entity. The goal is to obtain confidential data from the victims. Subsequently, the data are used for the realization of some type of fraud. To do this, the emails usually include a link that leads to counterfeit web pages. In this way, the victims enter the requested information that, in reality, will end up at the hands of the scammer. The main damages caused by phishing are identity and confidential data theft, loss of productivity, and misuse of resources (Reyes Neira 2015; Cordoba Bahamon 2016).

In general, phishing attacks are designed to obtain from the victim various valuable resources. These include personal or corporate data, which take advantage of email addresses, identification document numbers, and location and contact data; access to credentials, such as social networks and email accounts; and financial information, including credit card numbers, bank account numbers, and electronic commerce information. According to Monsalve (2018), some of the most common types of phishing crimes are:

- *Spear Phishing*: A type of phishing whose objective is a specific group of individuals or an organization. It is usually aimed at individuals or small groups. In this way, the campaigns are much more personalised and with a higher percentage of victims.
- *Whaling*: Aims for executives or ‘big fish’ in businesses. The targets of ‘cyberwhaling’ are mostly executives, preferably at the highest level, such as CEOs, CFOs, and other positions that involve high-level, decision-making people responsible for managing the finances and information of corporations.
- *Cloning*: This type of attack uses the impersonation of a legitimate email, delivered to the user's mailbox. The attached file or link within the malicious email is sent from a counterfeit email address that looks as if it comes from the original sender.
- *Phishing with geolocation*: Allows or denies access to a fake website in a certain country, through an IP address or proxy server. Any access that is made from another part of the world cannot access the phishing page. The objective is to make these attacks more effective, being more likely to reach specific victims and countries, in order to avoid being reported to authorities as malicious websites.

Malware execution

Cordoba Bahamon (2016) defines malware executions as malicious codes or software created to modify the usual behaviour of a program, to hinder or block a program’s functions, without the victim user being aware of the changes. Some of these take the form of viruses, worms, and Trojans (malware which misleads users of its true intent). According to Gómez Coronell (2014) banks are one of the most targeted organisations by cybercriminals. Some of the most common types of bank malware executed in Spanish with Hispanophone victims include:

- *Gataka:* a Trojan malware capable of using and manipulating online banking services. It is injected into the computer systems of organisations through explorer.exe files and infects computers. Once installed, the virus increases its functionalities by installing plugins, which make the virus more complex to detect. The Trojan maintains contact with a server, from which cyber-criminals can control the plugins

- *Zeus*: Also known as Zbot is a kit that allows cyber-criminals to create new malware to infect PCs. Hackers spread it to steal usernames and passwords, as well as other types of bank account access information
- *Gameover*: Steals online banking credentials. It is designed as a rootkit (computer software, typically malicious, designed to enable access to a computer while masking its existence, thereby making it difficult to eliminate). Gameover, unlike other Zeus-based Trojan programs, uses peer-to-peer technology for command and control instead of traditional servers; consequently, it is more resistant to disinfection attempts.
- *SpyEyes*: a software kit sold to cyber criminals. The cybercriminal who buys the kit can receive stolen online banking data. SpyEye also includes custom configuration files to attack most online banking websites. For example, additional fields, requesting information other than a username and password, can be added to a bank's website.

Reyes Neira (2015) and Info Spyware (2019) further defined other types of malware:

- *Trojans (Troyanos):* A Trojan is a small program usually hosted within another normal application (a file). Its objective is to go unnoticed by the user and to install itself in the system. After installing, it can perform the most diverse tasks, hidden from the user.
- *Worms (Gusanos)*: The main difference between worms and common viruses is their ability to survive without a host file. Worms can be reproduced using different channels, such as local networks, email, instant messaging programs, USB devices, and social networks.
- *Keyboard spies (Espías de Teclado):* Applications responsible for storing in a file everything the user enters through the keyboard (keyboard capturers). Keyboard spies can steal passwords and information on the equipment on which they are installed.
- *Botnets*: These constitute one of the main threats today. Botnets have appeared since 2004, increasing their appearance rates every year. A botnet is a network of computers infected by malicious codes, which are controlled by an attacker, making the affected computers work in a joint manner. When a computer has been affected by a malware of this type, it becomes a robot or zombie.
- *Adware*: A software that displays advertising material for different products or services. These applications show advertising in pop-up windows or through embedded pictures that appear on the screen pretending to offer different useful services for the user.

- *Hijackers:* Hijackers are responsible for hijacking the functions of web browsers by modifying the homepage and search bars of sites. They also block the navigation systems so that they cannot be restored by the user.
- *Rootkits*: Rootkits are able to perform several operations. This malware installs itself in an operating system, establishes communications with the attacker, and forces attacks in their hosting systems. If they are detected and attempts are made to eliminate them, they can cause problems to the operating system, including the inability to boot.
- *Rogues:* Rogue software is essentially a program that claims to be a program that it is not. With the proliferation of spyware, rogues emerged as an important product for cybercriminals interested in selling false antispyware, false optimisers, and false antiviruses. When being executed, rogues will inform the user about some false infection or false problem in the system that requires the user to buy a product, to remedy the issue.

Spyware deployment

Spyware consists of small programs that are installed on the system or computer, with the purpose of tracking personal data and an individual’s movements over the network. The information collected is sent to another server to be used for illegal purposes. Some types of spyware are found in internet sites that download malicious codes through ActiveX, JavaScript, or via cookies. They can also come in the form of viruses or Trojans and be hidden in free programs (Freeware)(Martínez 2018).

Normally, this software sends information to its servers, depending on the user's browsing habits. Also, spyware collects data about the websites that are browsed and the information that is requested on those sites, as well as IP addresses and URLs that are visited. This information is often the origin of spam and can be exploited for marketing purposes since it can be used to create statistical profiles on the habits of Internet users (Info Spyware 2019).

Card fraud

Card fraud includes purchases through credit or debit cards. Cards can be falsified, adulterated, stolen, or obtained illegally. Martínez (2018) states that the two most common cases of card fraud involve the supposed cardholder deceiving the merchant about his identity and cardholders using these cards at ATMs, either with adulterated or authentic cards but without authorization from the account holder, to obtain an economic benefit.

Ransoming

Ransomware is a type of malicious computer program that blocks, via encryption, access to all or part of the information contained in the computer. At this point, victims can become easy targets since the offender can request a ransom in exchange for removing the restrictions, essentially forcing the owner of the data to pay a ransom (Cordoba Bahamon 2016). In these cases, cybercriminals are not interested in one specific victim; rather, their attacks are done in bulk, with the aim of obtaining money from many victims. Such attacks are organised and involve people who are dedicated to different roles, such as developing the malware, infecting the systems, providing ‘customer service’ via forums or email, through which they indicate how much and how to pay for the rescue, and money laundering (Temperini 2018).

Other Transactional Cybercriminal Activities

Martínez (2018), López Sáenz (2014), and García Luna and Comenares Guillen (2015) further define other transactional cybercriminal activities:

Skimming: Are devices placed in ATMs, electronic purses, pin pads, Point of Sale (POS), and access doors. They fraudulently copy the magnetic stripes and the PIN of electronic cards and then clone or copy them.

Numerati: Involves an email or application program designed to track the movements of an individual over the network. When information is collected, it is then marketed to service, advertising, or statistical companies. In this way, users are redirected to other sites and encouraged to navigate through specific content for commercial purposes.

DDoS (denial of service attacks): Are attacks on a computer system or network that cause a service or resource to become inaccessible to legitimate users. Normally, the attacks cause the loss of network connectivity due to the consumption of the network bandwidth or the overload of the technological resources of the victim's system.

Arms and drug trafficking: Have used the internet for money laundering practices, for communicating and exchanging information on the authorities' actions against criminal organizations, and to expand the purchase and sale of narcotics and weapons worldwide.

Sexual exploitation: The Statistics of the Federal Preventive Police (PFP) of Mexico indicate that the sexual exploitation of minors through the internet is increasing rapidly. This crime ranks third, behind fraud and threats through cybernetic means.

Responses to Cybercrime

Argentina

Roibón (2019) notes that the economic losses caused by cybercrime are substantial with a tendency to increase in the short and medium term, and with developing countries being the most affected by this type of crime. In addition, The United Nations believe that developing countries 'lack the capacity to fight cyber-attacks and other forms of cybercrime'. Accordingly, victimization rates are higher in countries with lower levels of development. The lack of cooperation between developed and developing countries can also create safe havens for those who commit cybercrimes.

Sain (2015) finds that the low rate of judicial proceedings regarding this type of crime can be explained, in large part, by the economic, administrative, and technical behaviours of banks, companies, and internet service providers. When a user has experienced an economic loss through the use of computer devices, in most cases, the victim's main concern is to recover the lost money rather than pursuing the criminal prosecution of the perpetrator. Once victims realise that a third party has been granted unauthorised access to their bank accounts or credit cards to make purchases online, they register their complaints with the financial entity, and after a series of internal administrative mechanisms the money and access to their accounts and information are restored, in general because there are insurances that protect the customer, merchant, and financial provider. This represents only an administrative solution; in most cases, the victims do not file legal complaints for the criminal prosecution of the persons responsible for the crime.

Although the protection of information and other intangible objects or values existed already in the mid-twentieth century, the truth is that until recently protection has not been important. In the past decades, society has evolved from an industrial society to a post-industrial society; the value of information has increased in the economic, cultural, and political spheres; and the importance of information technology has increased. These changes have raised new legal problems and required new legal responses to information legislation (Sain 2013). Globally, the legislation is adapting to the changes that the world is experiencing as most of the crimes that existed in the non-digital world are transferred to the virtual world (Díaz et al. 2016).

Colombia

With the advancement of transactional mechanisms in the real and virtual world, it becomes increasingly complex for competent authorities to establish controls that guarantee the legality of the innumerable transactions of economic exchange. The strategies and mechanisms used by authorities are not always effective. For example, although virtual currencies serve as another mechanism to launder money through virtual platforms, when looking at Colombia, no specific regulation on the subject can be found (Palacios et al. (2015), cited in Quintero Porras (2016)). In addition, the continuous technological advances bring new security risks so long as the human resources do not have the training necessary to identify these types of attacks. Generating a culture of cybersecurity is important for the protection of personal data and the image of a company. Employers, employees, parents, and others need to develop safe habits so that they can be prepared to face cybercrime threats (Monsalve 2018).

In the case of organizations, whether industrial, financial, or health, Monsalve (2018) recommends the implementation of effective plans that focus on certain areas, people, roles, and functions within an organization, while maintaining a strong motivational aspect, demonstrating and giving the value that this type of sensitization deserves. For companies, related to and focused on technology and communications issues, these plans are a plus and a fundamental part in which all employees must participate.

From a more general perspective, Reyes Neira (2015) insists that cybercrime knowledge and prevention techniques are essential in protecting individuals against cyberattack:

- Thus, when giving away or selling a used cell phone, changing computer equipment, or lending a USB memory stick, sensitive data may be in danger; even after formatting these devices, they can be recovered by people with certain skills.
- Passwords and encryption must be used daily. People forget what they carry on their devices, and, only when they are victims of a robbery, they realise the extent to which they can be compromised by the information they loaded. Therefore, the first thing to do is to put a password to the removable disk used, to all electronic devices and laptops if possible, and enable an option so that information can be erased remotely.
- The first thing to always remember is the importance of sensitive information. On a personal level, this requires becoming aware of the data at hand and to learn how to take better care of it (i.e., by not leaving your cell phone or memory stick on the restaurant table or cybercafe within everyone's reach).

Mexico

The high growth of cybercrime in Mexico reflects how vulnerable this region is to cybercrime. Since Mexico ranks second after Brazil and before Columbia in Latin America for cyberattacks, Mexicans must demand that all governmental institutions address this issue immediately, given the exponential evolution of the technological instruments that allow dissemination and distribution of personal data online. There is a need to apply a comprehensive criminal policy due to the multi-offensive nature of cyber-attacks (Barba Álvarez 2017).

According to Avendaño Carbellido (2018), claims in Mexico for cyber fraud increased almost 800% from 2011 to 2016. This has to do with an increase in the number of operations carried out through digital banking or online frauds. However, when compared with the increase in traditional frauds, in the same period, the latter increased only slightly more than 30%.

Martínez López and Martínez López (2018) studied the awareness of young people to rights of privacy and data protection in Oxaca (Mexico). More than half of the students surveyed did not know that in Mexico there are specific laws that protect their personal data. A large part of the students in Oxaca did not know what ARCO rights are; were unaware of the institutions that focus on protecting their personal data, and did not know how to report improper processing of personal data.

In order for states to be effective in responding to the emerging demands that evolving activities, such as financial crimes, impose upon states, the analysis of cybercrime must include the processes of globalization. Rodríguez Mesa (2014) points out how these dynamics are played today between states, between states and non-state actors, and between states and large corporations. From that perspective:

- Criminological investigations and analyses must be held beyond national boundaries. The understanding of contemporary crime requires a comprehensive approach that allows understanding, integrating and underlining the different connections, generally worldwide, that characterise current crime. Research, that refers to a place - city, region or country and involves a single approach - generally sociological, can no longer explain what is happening in reality and consequently cannot offer a correct analysis of the problem or feasible solutions.
- The understanding of crime can no longer be based solely on explanations centred on the offender, the victim, and the circumstances surrounding the incident. In order to develop effective preventive measures, it is important to consider other variables

that play important roles in criminal processes, such as population mobility and immigration.
- States have the potential and ability to participate in, or have interests in, transnational criminal activities, such as clandestine immigration and arms or drug trafficking. Criminology cannot analyse globalised types of crime or propose solutions for change if it does not take into account the double role that governments may play in these scenarios.

Spain

The literature on transactional cybercrime in Spain indicates that, in general, Spain's normative framework and applicable laws and regulations against cybercrime are up to date. Moreover, Spain has effective institutions to combat money laundering and terrorist financing, has a high level of understanding of its risks, and has demonstrated significant achievements in the investigation and prosecution of money laundering. However, according to Braunschweig and (2016) various shortcomings prevent the criminal justice system from applying the required preventive and punitive measures. For instance, Braunschweig and (2016) notes that the deterrence and proportionality of the penalties for money laundering are of concern; the execution of selective financial sanctions against terrorism suffers from serious technical and practical deficiencies; the coordination of policies and operations to combat proliferation financing[71] is poor; and the applicable legal framework of the European Union regarding electronic transfers is fraught with deficiencies.

Criminal Proceedings to Cybercrime

Argentina

The Budapest Convention, the first international treaty to address internet and computer crime, sought to provide a basis upon which countries could establish national laws vis-à-vis cybercrime. Scholars such as Riquert (2014) believe that in general terms, the Argentinian legislation is compatible with the minimum standards that the conventions set forth.

Argentina has also enacted various laws which introduce, to the Criminal Code, new criminal types linked to the use of technology (Alcívar Trejo 2015). For example, Law 26388, enacted in 2008, addresses computer crimes. Law 26904 addresses grooming, a crime that affects a large number of minors, and Law 27436 criminalises the possession of child pornography, thereby modifying Article 128 of the Criminal Code (Parada and Errecaborde 2018).

Argentinian literature on the judiciary proceedings of digital crime is aware that the Argentinian legal framework revolves around the need to police specific actions, such as the need to regulate the fraudulent use of shopping cards in commerce or the need to penalise the manipulation of computer systems for economic gain to the detriment of the victims (Martínez 2018). However, for Sueiro (2014) the current regulatory system in the area of computer crime has multiple limitations in criminal matters, criminal proceedings, infrastructure, training of justices, and international cooperation. From that perspective, some criminal behaviours are still out of scope and need to be treated more comprehensively by the Argentinian laws and reforms on digital crime. Among these are the following:

- Cyber-occupation or improper registration of domain names,
- Spamming or junk mail or unsolicited advertising,
- Illegal collection and dissemination of data, images, and sounds, and
- The simple possession of child pornographic material.

Arocena (2012) claims that computer crimes are bound by their extraterritoriality, their timelessness, the intangibility of the instrument, and the object on which the conduct falls. As such, legislators must take these factors into consideration, so that they can create methods of investigation and clarification of the cyberelite which address these characters.

Colombia

Although Colombian lawmakers have been addressing transactional cybercrime, they have not fully addressed how these behaviours ought to be punished. Law 1273, of January 5, 2009, on the protection of information and data, modified the Colombian Criminal Code to create a new protected legal asset to preserve the systems that use information and communications technologies. As a result, the cybercrime that carries the greatest prison sentence in Colombia is theft by computer and similar means, which consists of overcoming computer security measures in order to obtain profit for oneself or for another, through the manipulation of a computer system, an electronic system network, telematics or other similar means, or by impersonating a user before established authentication and authorization systems (Parra 2016).

According to Quintero Porras (2016), this law is divided into two chapters. The first one, which involves “attacks on confidentiality, integrity, and availability of data and computer systems,” addresses abusive access to a computer system, illegitimate obstruction of a computer system or telecommunication network, the interception of computer data, computer damage, the use of malicious software, the violation of personal data, and the impersonation of websites to capture personal data. The law also addresses punitive measures, increasing their severity by 50% to 75%, when the crime is committed:

- On networks or computer systems, via state or official communication platforms, or national or foreign communication systems;
- By a public servant while at the workplace;
- By taking advantage of the trust placed by the holder of the information or by those who have a contractual link with it;
- By revealing or disclosing the content of the information to the detriment of another;
- To acquire a profit for oneself or for a third party;
- For terrorist purposes or to generate risk to national security or defence; or
- By using a third party in good faith.

The second chapter of the aforementioned law, entitled ‘On computer attacks and fractions’, establishes the following crimes by defining theft via ICT systems and the compromise of ICT systems. Quintero Porras (2016) maintains that behaviours, such as money laundering through virtual currencies, will be difficult to associate with the above conditions. As a result, punishing rapidly evolving transactional cybercrimes remains a challenge for the Colombian state (Quintero Porras 2016).

Mexico

According to the Council of Europe (COE) (2019), Mexico does not have an independent law that addresses the investigation and prosecution of cybercrime offenses. This is consistent with the limited resources allocated to cybercrime in Mexico. Nonetheless, the COE (2019), the Federal Criminal Code, the Federal Law against Organized Crime, and other federal and state criminal laws contain provisions that sanction and punish offenses committed through and against the use of computer systems. These include illegal access, modification or destruction of information of computer systems, possession, sale and distribution of child pornography, promotion and facilitation of sexual tourism, and offenses against the security of the nation, such as espionage, rebellion, and terrorism. During the Workshop on Cybercrime, held in Mexico City on March 31, 2014, the government of Mexico voiced its commitment to working with federal agencies and branches, including the Office of the Attorney General and the Ministry of Foreign Affairs, to modify the Federal Criminal Code so that it would include new punishments and offenses related to cybercrime. For example, through Reform 75 of the Federal Criminal Code 1999, Articles 211 (bis 1) to

211 (bis 7) were enacted. These criminalise specific computer crime behaviours (i.e., Illegal access and the use and copying of information contained in systems, equipment, or storage devises pertaining to the state (Temperini 2013).

Although the Federal Government has implemented new measures to criminalise and punish such criminal activities, according to Kobek (2017), ‘there is still a long way to go with respect to these laws. Some areas of opportunity will require the government to cooperate with private institutions, as well as with international organizations to make the laws more effective and reduce the risks of new criminal agents in cyberspace’.

Spain

According to Muñoz (2018), the lack of digital literacy programs in Spain reduces the possibilities of articulating a supra-state legal framework capable of guaranteeing reasonable expectations of privacy to the millions who use cyberspace. As a more sophisticated culture of privacy evolves and consolidates, regulatory bodies at the state and supranational levels need to adopt measures that assure that the rules of fair play pertaining to cyberspace are also applied to new scenarios.

However, to establish a consistent methodology that allows combating cybercrime, the punitive system must take into consideration computer crimes. For example, the Spanish Criminal Code, Law 10 of 1995, does not contemplate or define ‘computer crimes.’ Instead, the criminal code relies upon other regulations and definitions. Hence, although Law 5 of 2010 and modified Law 10 1995 of the Criminal Code do not expressly define computer crimes, they do refer to computer manipulations and scams (Muñoz 2018).

Although Spain still needs to adjust its criminal justice system to address the requirements of a constantly evolving culture of cybercrime in Europe and the world, important milestones described by Anguita Osuna (2018) in the fight against cybercrime have been achieved. An important initial step Spain’s 2010 ratification of the Budapest Convention.

In 2001, the Council of Europe recommended the introduction of a 24-hour uninterrupted service to fight crime in the field of high technology. In 2004, the European Parliament and the Council supported the creation of the European Network and Information Security Agency. In 2007, the European Commission called for a general policy to combat cybercrime and defined cybercrime ‘as criminal activities carried out with the help of communications networks and electronic information systems or against such networks and systems’. Another important milestone in the fight against cybercrime was the communication of the 2009 European Commission entitled ‘Protecting Europe from cyber-attacks and large-scale disruptions: increasing preparedness, security and resistance". This communication defined a plan of immediate measures to enhance the security and resistance of critical information infrastructures. Yet another key element to fight computer crime was the European Cybercrime Center (EC3), created in 2013 as part of Europol.

Further milestones described by Anguita Osuna (2018) include the approval of the 2013 Directive on Attacks on Information Systems, whose purpose is to:

> approximate the criminal law norms of the Member states regarding attacks against information systems, through the establishment of minimum standards relating to the definition of criminal offenses and applicable sanctions -to cybercrime-, and to improve cooperation between competent authorities, including the police and other specialized services responsible for law enforcement in the Member states, as well as specialized bodies of the Union, such as Europol and the European Cybercrime Centre and the European Union Agency for Network and Information Security (ENISA).

Conclusion

The continuous emergence of technological developments at a global scale has contributed to increased participation in cybercriminal activities. The Hispanophone literature, that studies cybercrime scenarios in a Hispanophone context, acknowledges the capacity of criminals to use new developments, such as cryptocurrencies, to engage in various illicit activities, including sex offending, money laundering, and financial crime. From a transactional perspective, the Hispanophone literature has identified several critical activities that affect the economic activities of individuals and organisations. This report has offered a comprehensive review of four major aspects of transactional cybercrime from a Hispanophone perspective: main transactional cyber-activities and behaviours, regulation bodies including national cybercrime strategies, government responses, and crime proceedings. The analysis was performed in four major, Spanish-speaking countries with a high population of Internet users: Argentina, Colombia, Mexico, and Spain.

These four countries hold a coherent national cybersecurity strategy. As each country experienced increased online use, the respective governments have delivered a prompt cybersecurity strategy in line with the criminal and technological challenges present in their own region and have aligned themselves with the highest international standards on cybersecurity. In general, the national cybersecurity strategies of the Hispanic countries studied herein present a clear scheme comprised of various objectives and sub-strategies that seek to address important topics, including training and education of the public and private actors; improving regulatory frameworks, norms, and regulations; enhancing international cooperation; improving the technological capacities of governmental institutions to protect and defend cyberspace; generating a culture of cyber-awareness where individuals, and private and public agents understand the risks and challenges in the use of cyberspace; promoting inclusion and respect for the diversity of users of cyberspace, including the vulnerable people, such as young people; promoting research and technological developments that through innovation processes allow for the protection of the national cyberspace; and improving the capacity of the criminal justice system to enhance its capacity to proceed on crime matters perpetrated in cyberspace.

With the exception of Mexico, which leads in Latin America for its steps towards cryptocurrency regulation, none of the other countries studied has clear regulations or prosecuting bodies against transactional cybercrime. In each country, the financial bodies that regulate financial activities clearly note that virtual currencies are neither regulated by law, nor subject to the control, surveillance or inspection of these public agencies. Although the governmental response has been rapid and there is a strong interest in developing regulations that cope with the technological threat that cybercrime presupposes in the region, government agencies lack the capacity to exercise law enforcement since they cannot respond adequately and effectively to financial cybercrimes and cannot prosecute financial cybercrimes effectively in light of a lack of clear normativity and legislation.

In terms of responses, the technological limitations of countries in Hispanophone regions present an opportunity for cybercriminals to establish safe havens. Poor policies and education in both the public and private sectors allow for slow responses that rarely provide solutions to victims of financial cybercriminals. The lack of a culture of cooperation among agencies, localities, and countries in the Hispanophone region presents a challenge for individuals and institutions that are not working under a culture of integration and collaboration, especially considering the interconnectivity characteristics of the cyberworld. In terms of criminal proceedings, the laws pertaining to financial cybercrime of countries in this region were constructed under a framework that did not consider the technological advances of the new world. In general, the legislation has adapted new decrees and regulations in an attempt to prosecute circumstances and activities that were inexistent more than twenty years ago. That is the case in Argentina where its legal system requires a deep revision on important aspects, such as unsolicited advertising, including spam, and the possession of child pornographic material. In Colombia, acts of money laundering have occurred through the use of cryptocurrencies, which the law has not been able to successfully prosecute due to the limitations of its laws.

Works Cited

ABC. 2018. "El CNMV reclama competencias para regular las criptomonedas." Accessed 14 December 2019. https://www.abc.es/economia/abci-cnmv-reclama-competencias-para-regular-criptomonedas-201807041548_noticia.html.

Alcívar Trejo, Carlos ; Alvarez Domenech, Gustavo Arturo ; Chimbo Ortiz, Karla Maribel 2015. "La Seguridad Jurídica Frente a los Delitos Informáticos." *Avances* 10 (12): 41-41.

Anguita Osuna, José Enrique 2018. "Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea." *RESI: Revista de estudios en seguridad internacional* 4 (1): 107-126.

Arocena, Gustavo A. 2012. "La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional." *Boletín Mexicano de Derecho Comparado* (135): 2.

Avendaño Carbellido, Octavio. 2018. "Los retos de la banca digital en México." *Revista IUS* 12 (41): 87-108.

Barba Álvarez, Rogelio. 2017. "El robo de identidad en México." *Dikê: Revista de Investigación en Derecho, Criminología y Consultoría Jurídica* (22): 245-260.

Braunschweig, Maximiliano; Castro, Romina; García Fernández, Simón; Pugh, Rocío; Margoni, Julieta, and 2016. "Lavado de activos en Argentina y España: comparación normativa aplicable y el rol del contador." *Universidad Argentina de la Empresa*: 1-71.

Colombia Fintech. 2019. "Colombia da el primer paso para regular Bitcoin." Accessed 16 December 2019. https://www.colombiafintech.co/novedades/colombia-da-el-primer-paso-para-regular-bitcoin.

Comisión Nacional Bancaria y de Valores - Government of Mexico. 2019. "¿Qué hacemos?". Accessed 12 December 2019. https://www.gob.mx/cnbv/que-hacemos.

Cordoba Bahamon, José Antonio. 2016. "Malware: una puerta a la cibercriminalidad." *Universidad Piloto de Colombia*: 1-8.

Credimarket. 2013. "¿Qué organismos regulan el sistema bancario español?". Accessed 15 November 2019. https://www.credimarket.com/finanzas/que-organismos-regulan-el-sistema-bancario-espanol/2013/09/05/.

Criptodinero. 2019. "Regulación de las criptomonedas en Argentina." Accessed 15 December 2019. https://criptodinero.es/legislacion/regulacion-de-las-criptomonedas-en-argentina/.

Díaz, Francisco Javier, Paula Venosa, Nicolás Macia, Einar Felipe Lanfranco, Alejandro Javier Sabolansky, and Damián Rubio. 2016. "Análisis digital forense utilizando herramientas de software libre." XVIII Workshop de Investigadores en Ciencias de la Computación (WICC 2016, Entre Ríos, Argentina).

Diaz, J, and A Pinto. 2014. "Reflexiones a partir de las posibilidades y riesgos de las TIC: caso práctico en la experiencia En TIC Confío en La Guajira-Colombia." Extraído de: Congreso Iberoamericano de Ciencia, Tecnología, Innovación y Educación buenos aires Argentina noviembre, Buenos Aires.

El Economista. 2019a. "¿Cómo regulará Banxico las criptomonedas?". Accessed 15 December 2019. https://www.eleconomista.com.mx/sectorfinanciero/Como-regulara-Banxico-las-criptomonedas-20190214-0114.html.

---. 2019b. "El debate por la regulación de las criptomonedas llega al Senado argentino." Accessed 15 December 2019. https://www.eleconomista.com.ar/2019-11-el-debate-por-la-regulacion-de-las-criptomonedas-llega-al-senado-argentino/.

Externado University. 2019. "Las criptomonedas y su marco normativo en Colombia." Accessed 12 December 2019. https://derinformatico.uexternado.edu.co/las-criptomonedas-y-su-marco-normativo-en-colombia/.

FATF. 2010. *Combating Proliferation Financing: A status report on policy development and consultation*. Paris: The Financial Action Task Force.

García Luna, Julio Cesar , and Luis Enrique Colmenares Guillen. 2015. "Pornografía y explotación sexual infantil, efectos sociales y la tecnología." *Visión Criminológica-criminalística* (April-June).

Gobierno de España. 2013. Estrategia de Ciberseguridad Nacional. edited by Departamento de Seguridad Nacional - Presidencia de Gobierno.

Gómez Coronell, Olimary. 2014. "Estrategias de la seguridad de la Información para combatir el Fraude Bancario en Colombia." *Universidad Piloto de Colombia*: 1-10.

Government of Mexico. 2017. Estrategia Nacional de Ciberseguridad. Mexico.

Hernández, José Carlos. 2018. "Estrategias Nacionales de Ciberseguridad en América Latina." *Grupo de Estudios en Seguridad Internacional GESI* Análisis 8: 1-8.

Humar, Fabio Andrés. 2008. "Estructura del sistema financiero argentino." *Revista de la Maestría en Derecho Económico* 4 (4): 63-90.

Info Spyware. 2019. "¿Qué son los malwares?". Accessed 17 December 2019. https://www.infospyware.com/articulos/que-son-los-malwares/.

Kobek, Luisa Parraguez. 2017. "The State of Cybersecurity in Mexico: An Overview." *Mexico Institute. https://www.wilsoncenter.org/sites/default/files/cybersecurity_in_mexico_an_overview.pdf*: 1-23.

López Sáenz, Manuel E. 2014. "De propósitos y despropósitos, usos y desusos: hacia la gobernanza de internet." *RevIISE-Revista de Ciencias Sociales y Humanas* 6 (6): 35-46.

Martínez López, Norma, and Roselia Martínez López. 2018. "Los jóvenes y la ciberseguridad en zonas rurales del Estado de Oaxaca. Caso: Instituto de Estudios de Bachillerato del Estado de Oaxaca (IEBO), plantel 165." *RECAI: Revista de Estudios en Contaduría, Administración e Informática* 7 (20): 14-35.

Martínez, Matilde. 2018. "Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil." In *Cibercrimen y Delitos Informático*, edited by RA Parada and JD Errecaborde. Buenos Aires, Argentina: Erreius.

Martínez Moya, Carlos Andrés. 2016. "Los desarrollos tecnológicos y su influencia en el crecimiento de los ciberdelitos en Colombia." *Universidad Piloto de Colombia*: 1-8.

Meseguer González, JD. 2013. "Los Nuevos Modi Operandi de los Ciberdelincuentes Durante la Crisis Económica." *Revista de Derecho UNED* (12): 495-523.

MinTIC. 2014. Agenda Estratégica de Innovación: Ciberseguridad. edited by Ministerio de Tecnologías de la Información y las Comunicaciones. Bogotá D.C. : CINTEL.

Monsalve, Jaime. 2018. "Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos)." *Universidad Piloto de Colombia*: 1-10.

Muñoz, Miguel Moreno. 2018. "Virtualización del espacio público y concepto débil de privacidad. Lecciones del caso Facebook-Cambridge Analytica." *Ensayos de Filosofia* S2, 8 (3): 1-11.

Parada, RA, and JD Errecaborde. 2018. "Prólogo." In *Buenos Aires: Erreius*, edited by RA Parada and JD Errecaborde. Buenos Aires, Argentina: Erreius.

Parra, Jaime Hernán Rojas. 2016. "Análisis de la penalización del cibercrimen en países de habla hispana." *Revista Logos, Ciencia & Tecnología* 8 (1): 220-231.

Pérez, Hannah 2019. "Todo sobre Bitcoin y las criptomonedas en México." Accessed 12 December 2019. https://www.diariobitcoin.com/index.php/2019/09/29/todo-lo-que-debe-saber-sobre-bitcoin-y-las-criptomonedas-en-mexico/.

Pérez López, Xesús. 2017. "Las criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España." *Revista de Derecho Penal y Criminología* 18: 141-187.

Presidencia de la Nación. 2019. "Comité de Ciberseguridad - Decreto 577/2017." Accessed 22 November 2019. http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm.

Quintero Porras, Carlos Oscar. 2016. "La acción delictiva a través de la informática en Colombia: el caso particular del lavado de activos y la lucha institucional contra su configuración." *Universidad Católica de Colombia*.

República Argentina. 2019. Estrategia Nacional de Ciberseguridad de la República Argentina. República Argentina.

Revista Pensamiento Penal. 2018. "Criptomonedas. Robo." La sala unipersonal N° 3 de la Cámara Tercera en lo Criminal de Resistencia. Cámara Segunda en lo Criminal de Resistencia. Accessed 12 December 2019.

Reyes Neira, Juan Manuel. 2015. "Ciberdelincuencia una realidad virtual contada a medias." *Universidad Piloto de Colombia*: 1-8.

Reygadas, Luis. 2018. "Dones, falsos dones, bienes comunes y explotación en las redes digitales. Diversidad de la economía virtual." *Desacatos* (56): 70-89.

Riquert, Marcelo. 2014. "Convenio sobre Cibercriminalidad de Budapest y el Mercosur. Propuestas

de derecho penal material y su armonización con la legislación regional sudamericana." In *Delitos Informáticos*, edited by Alejandro Alagia, Javier A. De Luca and Alejandro Slokar, 107-180. Buenos Aires.

Rodríguez Mesa, María José 2014. "Nuevos lineamientos en Criminología." *Archivos de Criminología, Seguridad Privada y Criminalística* (12): 1-10.

Roibón, María Milagros 2019. "La estafa informática en el código penal Argentino." *Revista Pensamiento Penal*.

Sain, Gustavo. 2013. "El Derecho Penal aplicado a los delitos informáticos: Una política eficiente para el cibercrimen?" *Revista Pensamiento Penal*.

---. 2015. Tercer muestreo de denuncias judiciales de la República Argentina. edited by Secretaría de Justicia. Buenos Aires, Argentina: Presidencia de la Nación.

---. 2018. "La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal." In *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*, edited by RA Parada and JD Errecaborde, 7-32. Buenos Aires: Erreius.

Sueiro, Carlos. 2014. "La criminalidad informática en el Anteproyecto de Código Penal de la Nación." In *Delitos Informáticos*, edited by Alejandro Alagia, Javier A. De Luca and Alejandro Slokar, 189-234. Buenos Aires.

Superintendenca Financiera de Colombia. 2019. "Acerca de la SFC." Accessed 16 December 2019. https://www.superfinanciera.gov.co/inicio/nuestra-entidad/acerca-de-la-sfc-60607.

Temperini, Marcelo 2013. "Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte." 1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información, National Technological University, Córdoba.

---. 2018. "Delitos informáticos y cibercrimen: alcances, conceptos y características." In *Cibercrimen y Delitos Informáticos*, edited by RA Parada and JD Errecaborde. Buenos Aires: Erreius.

Territorio Bitcoin. 2019. "La CNMV avisa sobre ciertos exchanges de criptomonedas. ¿Que significa para los traders?". Accessed 12 December 2019. https://www.territoriobitcoin.com/la-cnmv-avisa-sobre-ciertos-exchanges-de-criptomonedas-que-significa-para-los-traders/.

Section V: Lessons from the Francophone Literature

Introduction

The cybercrime literature has grown exponentially in response to emerging and evolving threats facilitated by the digital environment. While cybercrime is increasingly becoming subject to empirical studies, only a subset of these have focused on the financial dimensions of cybercrime, and even fewer have examined how offenders profit or ‘cash out’ from their crimes. Nonetheless, the literature on cybercrime clearly establishes the central role of fiat and virtual currencies in the monetization of crimes. Consequently, understanding the behaviours of individuals who use the digital environment to facilitate criminal offending requires an understanding of how the financial infrastructure influences these offences.

This report details the state of the knowledge in the French cybercrime literature. The first section of this report discusses the methodology used to conduct the review and locate relevant articles. The second section of the report provides an overview of the government bodies, private sector agencies, and academic and think tank organizations involved in countering cybercrime. The third section details the results from the review, highlighting what we know about the cybercrime ecosystem, the financial infrastructure used by individuals involved in these offences, and the effectiveness of private and public sector responses to disrupt these ecosystems. For each subsection, we provide a summary of the main findings, gaps in the literature, and ways to move forward.

Methods

This report focuses on French-language sources. It provides a systematic review of extant research on criminal transactional methods in cyberspace conducted in the French language and studies in the English language that cover the French context. The objective of the review is to summarise the state of knowledge within the area of criminal transaction methods, as summarised by francophone researchers. Because little research has been conducted on illicit transactional methods, particularly online and in the French language, we will draw from various sources, including conceptual essays, policy analyses, white papers, and empirical analyses. In addition, we include books and book chapters on these issues, scientific articles, and government and think-tank reports. Consistent with the English review, we only retrieve articles, books, book chapters, and relevant reports that are accessible through our university system and that have been published in 2013 or afterwards.

To capture a wide range of literature that examines illicit transactional methods in cybercrime, four strategies were adopted. First, a keyword search, using relevant citation databases, including the French Google Scholar indexing database, was conducted. Google Scholar covers academic work and other “grey” literature that may not be captured in standard academic citation index databases; it also allows us to limit the searches to French results. We use similar keywords as the English review: Cybercrime; Cybermenace; Cyberattacque; Darkweb; Darknet; Digital; En ligne; Internet; Botnet; Bulletproof; BPH; C2; Casino; Contrefaire; Attaque par déni de service; DDOS; Extortion; Falsifier; AML; Anti-blanchiment d’argent; Hack; Rançon; Passeurs d’argent; Violation de système; Intrusion de système; Bitcoin; Institutions financières; Fintech; P2P; Paypal; QR; Transaction. In addition, for all the articles retained from the search strategy, we reviewed all literature cited in their reference lists and all the studies which cited the article, to get the most up to date reports and articles.

Second, we searched relevant francophone cybercrime and criminology journals using the same search terms as above. The journals involved included *Criminologie*, *Criminologie et droit pénal*, *Crimino Corpus*, *Champ penal*, *Revue internationale de Criminologie et de police*, *Revue canadienne de criminologie et de justice pénale*, and *Revue française de criminologie et de droit pénal*. Third, we conducted targeted searches among government agencies, think tanks, and non-profits in French countries with more than 20 million Internet Users, which include Canada and France. In Canada, this includes provincial centres, such as Quebec law enforcement agencies. Internationally, we also identified French cybercrime organizations, including Francopol – Réseau international francophone de formation policière – and the Forum international de la cybersecurité. Fourth, the keyword searches were complemented with a systematic examination of curriculum vitaes of well-known francophone scholars involved in research on illicit transactional methods in cyberspace, such as Benoit Dupont and David Décary-Hétu in Canada, and Quentin Rossy in Switzerland.

The search yielded 65 peer-reviewed articles, books, book chapters, reports, and white-papers. In the following review, we retained 37 of them, focusing on studies that used empirical data or conceptual pieces that provided novel insights into the financial infrastructure of cybercrime. Studies were excluded if they lacked empirical data, consisted of broad overviews, and/or did not provide support to justify claims.

The State of Play in French Regions of Focus: Law Enforcement Bodies, Socio-political Considerations, and Known Trends

This section provides an overview of the relevant cybercrime regulations and bodies involved in two major French speaking regions with a high population of Internet users: the province of Quebec in Canada and France.

Québec, Canada

Cybercrime

The French speaking province of Quebec, Canada, represents a major hub for centres and non-profit organizations that aim to counter cybercrime. These include the Centre of Excellence hosted at the University of Montreal (Serene-Risc), a non-profit industry cluster (In-Sec-M), a public-private partnership (CyberEco), and a government body dedicated to combating financial crime (The Financial Markets Authority). These agencies work in tandem with other centres throughout Canada, and thus complement the network of cybercrime bodies that were outlined in the English report.

- **Serene-Risc, Smart Cybersecurity Network-Réseau Intégré sur la cybersécurité**. Established in 2014, Serene-Risc is funded by the federal government under the Networks of Centres of Excellence of Canada. Serene-Risc aims to enhance knowledge mobilization in the realm of cybersecurity by bridging the divide between academics and practitioners. To accomplish this objective, Serene-Risc engages in four key activities: i) holding annual workshops across academic, industry, and government agencies to present updated research findings and to highlight key cybersecurity issues, ii) providing quarterly newsletters that summarise the latest research findings across the cybersecurity literature, iii) maintaining an online blog, *Konnect,* which provides up to date research summaries, and iv) providing a professional development program for young professionals and graduate students to develop their skills and work on cybersecurity projects at Serene-Risc in Montreal. Overall, the Centre provides a platform for information exchange among agencies that may otherwise be disconnected, creating a coherent platform for preventing and countering cybercrime. Since its inception, the Centre has partnered with over 25 private and public agencies across Canada, including Canada's federal law enforcement body (the Royal Canadian Mounted Police), local law enforcement agencies, and the National Bank of Canada.

- **In-Sec-M, Innovation, Security, Marketplace.** In-Sec-M was created in 2017 as a Digital Centre of Excellence funded in part by the Digital Economy Action Plan of the Ministry of Economy, Science and Innovation of Quebec (MESI). In-Sec-M has similar objectives to Serene-Risc, aiming to increase the cohesiveness of the Canadian cybersecurity agency by bringing together the private sector, research centres, and academics. The Centre also provides funding for projects related to cybersecurity and works with Serene-Risc to host cybersecurity forums for academics and practitioners.
- **CyberEco.** CyberEco is a non-profit agency created in 2018 by four firms involved in the financial, engineering, and accounting sector. The agency, based in Montreal, aims to make Quebec a global leader in cybersecurity by accelerating workforce development of cybersecurity experts and educating individuals and businesses about cybersecurity risks. The agency is relatively small in scope compared to agencies such as Serene-Risc, with fewer partners, but has the support of major industry partners, such as IBM.

1.

Financial Crime

The Financial Markets Authority (AMF) is Quebec's provincial agency for regulating its financial sector. In addition, Quebec has provincial (Sûreté du Québec) and municipal (e.g., Montreal Police Service, SPVM) law enforcement agencies that are responsible for directing investigations into illicit financial and cybercrime incidents. These investigations may be carried out independently or in collaboration with the AMF. However, law enforcement agencies offer little publicly available information on their activities or investigations pertaining to cybercrime.

- **AMF, The Financial Markets Authority (Autorité des marchés financiers).** The AMF was established in 2004 under the *Act respecting the Autorité des marchés financiers* (respecting the regulation of the financial sector), designed to regulate the financial sector. The AMF is mandated by the Quebec government to regulate the financial markets within the province. Consequently, the AMF oversees various areas, including the distribution of financial products and services. As part of its mandate, the AMF is involved in fraud prevention, which includes educating the general public on recognizing, avoiding, and reporting financial fraud. The AMF provides a reporting service to the public, which includes an online portal for the public to report frauds.

The province of Quebec provides a unique context for examining the regulation of virtual currencies. The province implemented its own laws for regulating virtual currencies that are distinct from the rest of Canada. Specifically, the Money-Services Business Act mandates that automated teller machines (ATMs), including those for Bitcoin or other digital currencies, be licensed with the AMF. The AMF processes these licenses, providing the agency with detailed information on both the business operators as well as the individuals who use these services. The licensing procedure requires that businesses submit detailed information on their operations, including a list of the financial institutions they are linked with, a list of the owners, managers, employees, and a business plan. In addition, the AMF requires that licensed businesses keep records of all transactions, which means that each business must record information on all its clients, which then can be inspected by the AMF. Thus, the AMF is uniquely positioned to exercise more control over the surveillance of points of entry and exit of digital currency within the province (Ivelin 2016).

France

France has consistently identified cyberattacks as a major threat to the nation-state. The country developed a cybersecurity strategy in 2010, which was published shortly after the detection of a cyberattack to spy on the economic and finance ministries. The state cybersecurity agency has identified attackers who target vital digital infrastructure; in particular, their defence, health and digital research centres are their biggest priority. In 2018, the French state’s cybersecurity agency reported 1,869 cyberattacks, including 16 major incidents and 14 that involved cyber defence operations (ANSSI 2018). Most cyberattacks in France are financially motivated, with fraud being the most common attack type, including phishing, ransom attacks, and attacks stealing personal data. France also has been identified as having the highest number of cyber victimizations than any other country in Europe, attributed to the French population’s greater access to the Internet.

Cybercrime

France has made cybercrime a national priority, as evidenced by the scope of its involvement in international initiatives, and the development of numerous state agencies responsible for countering cybercrimes. In 2017, the Minister for Europe and Foreign Affairs published the French National Digital Security Strategy, which outlines five objectives of the French State: i) a commitment to defend interests in cyberspace and reinforce security of its digital infrastructure by enhancing its cooperation with the private sector, ii) greater vigilance in the handling of personal data, iii) enhancing awareness of school children and students about digital risks, and training the public and private sectors in cybersecurity prevention and risks, iv) supporting investment in French businesses involved in providing secure digital products and services, and v) playing a greater role in international cybersecurity bodies, while assisting the least-protected countries in building their cyberspace infrastructure (Secretariat-General for National Defence and Security, 2015).

France plays key roles in international initiatives to combat and regulate cybercrime. France has worked within the United Nations on international cybersecurity issues. In 2016, France, with NATO, adopted the 28 Nations of a Cyber Defence Pledge, and, with the G7, France is working towards complying with the G7 Declaration on Responsible States Behavior in Cyberspace. In addition, France belongs to the major cybercrime conventions, including the 2001 *Convention on Cybercrime*, more commonly referred to as the Budapest Convention, and recently led the *Paris Call for Trust and Security in Cyberspace in 2018.* The Paris Call outlines nine goals to establish international norms for the Internet, including the disclosure of digital vulnerabilities, defence against foreign actors from interfering with electoral processes, and the prevention of the private sector from retaliating against cyberattacks (ANSSI 2018). The Paris Call has been endorsed by more than 50 countries, as well as multiple nonprofits and private corporations. The Paris Call is also reflective of France’s efforts to work closely with private companies to combat cybercrime.

In addition, France is a partner of the Joint Cybercrime Action Taskforce (J-CAT). J-CAT was launched in September 2014 and is led by Europol’s Cybercrime Centre, EC. J-CAT is a collaboration among participating EU Member States that was established in response to cross-border activities of cybercrime and provides a platform for participating Member States to collaborate across borders and coordinate international investigations. Because J-CAT is an independent Member State initiative, it also allows members to work with non-member states through ad-hoc proxy agreements, providing flexibility to respond to international cybercrimes that may emerge in non-Member States (Reitano et al. 2015).

France also has multiple levels of government that prioritise cybersecurity, including a national cybersecurity agency, agencies within the Armed Forces, as well as national and municipal law enforcement investigative bodies dedicated to combating cybercrime. Moreover, France's government has fostered the domestic cybersecurity industry through multiple research centres and private-public partnerships that aim to counter cybercrime. Finally, it has worked bilaterally with French speaking countries in Africa to improve their cybersecurity infrastructures.

- **ANSSI, The National Cyber Security Agency of France (***Agence nationale de la sécurité des systèmes d'information***).** ANSSI was established in 2009 as part of the Secretariat-General for National Defence and Security. ANSSI acts as France's 'first responder' to attacks in the French cyberspace. The agency has approximately 600 employees and is responsible for protecting the State's information security digital systems, as well as detecting and responding to computer attacks, with a focus on those pertaining to the French state. ANSSI also plays a key role in knowledge mobilization, publishing annual reports, and bringing together academic and government publications on a centralised platform.[72]
- **CERT-FR, Computer Emergency Response Team – FR.** (*Centre gouvernemental de veille d'alerte et de réponse aux attaques informatiques*)**.** CERT-FR was established in 2000 to protect the State network against attacks. CERT-FR's main mission is to monitor and respond to computer attacks by reinforcing and preventing intrusions into information systems dealing with the nation-state's administration.[73] CERT-FR works with ANSSI and aims to provide complementary preventative activities to those offered by the agency. CERT-FR provides services 24/7 and is also responsible for maintaining a security alert system that reports all detected vulnerabilities and cyberattacks dating back to 2000 (available at https://www.cert.ssi.gouv.fr/alerte/).
- **COMCYBER, Cyberdefense Command** (*Commandement de la cyberdéfense*). COMCYBER was established in 2017 and is part of the French Ministry for the Armed Forces. COMCYBER is in charge of i) protecting the Armed Forces Digital Networks and ii) integrating digital warfare into its own operations.

In France, the two national law enforcement bodies have units that are directly responsible for countering cybercrime. The SDLC represents the cybercrime unit within the French National Police, and the Centre de lute contre les criminalités numériques (C3N) is the cybercrime unit within the National Gendarmerie.

- **SDLC, Sub-directorate for the Fight Against Cybercrime (***Sous-direction de Lutte contre la Cybercriminalité***).** The SDLC is part of the National Police and represents one of the five main sub-directorates under the Police's Judicial Directorate. The SDLC was established in 2014 and comprises of more than 130 personnel, of which 10 are engineers and technicians.[74] The aim of the SDLC is to combat cybercrime through preventative and repressive measures. The SDLC can be divided into five main bodies: i) The Office of Strategic Coordination, that is responsible for the internal and external communications regarding the fight against cybercrime; ii) the Internet Office that collects information pertaining to Internet Service Providers and interventions for the benefit of investigators in the National Police; iii)The Office of Training in the Fight Against Cybercrime that coordinates the initial training and development of cybercrime investigators; iv) The Central Office for the Fight against Crime related to Information and Communication Technology (OCLCTIC), one of the main investigative bodies to intervene and investigate perpetrators of technological crimes and disseminating information on cybercrime infractions to all law enforcement agencies; and v) Division in Charge of Anticipation and Analysis, that proactively monitors cybercrime and provides technical services for judicial investigations.

- **C3N, Digital Crime Centre** (*The Centre de lute contre les criminalités numériques*). The C3N was established in 1998 and is part of the National Gendarmerie, France's national police force and branch of the French Armed Forces under the jurisdiction of the Ministry of the Interior. The Centre has three main objectives: i) conduct judicial investigations based on complaints made directly to the agency and reports made by investigators who are proactively monitoring the clearnet, darknet, and peer-to-peer networks; ii) conduct criminal intelligence and operational support, including real-time assistance for investigations; and iii) provide permanent surveillance of the Internet. The agency provides a hotline for investigators for assistance in cybercrime incidents.[75]

In addition, municipal police forces have their own cybercrime divisions for investigating incidents that occur against their own infrastructure.

- **BEFTI, Information Technology Fraud Investigation Brigade** (*La Brigade d'enquêtes sur les fraudes aux technologies de l'information*). BEFTI was created in 1994 and consists of approximately 25 specialised police officers who investigate cybercrime incidents related to Paris. Under the direction of The Police Prefecture of Paris, BEFTI includes both police officers and cybercrime investigators who are in charge of investigating diverse cybercrime infractions, including stolen data, telephone hacking, website defacement, counterfeit software, and computer intrusions. The specialised officers are split into three groups, two of which are involved in investigations and one in assistance.[76]

- **PICyAn, Cybercrime Investigation Platform and Digital Analysis**. PICyAN is a police service which is specialised in analysing the IT equipment acquired during police seizures and Internet surveillance.

France also has established a host of Centres of Excellence and private-public partnerships that aim to counter cybercrime.

- **CECyF, Expert Centre Against French Cybercrime** (*Centre Expert contre la* **Cybercriminalité Français). The CECyF started in 2010 as the** 2Centre project (Cybercrime Centre of Excellence Network for Training, Research, and Education). Its goal was to create a network of Cybercrime Centres of Excellence for Training, Research, and Education that would bring together law enforcement, academia, and the private sector to combat cybercrime. Since the Centre's development in Ireland and France, it has expanded to include other countries, such as Belgium, Bulgaria, England, Estonia, Greece, Lithuania, and Spain. The 2Centre project which ran from 2010 to 2013 evolved into the CECyF (also referred to as the F-CCENTRE) in 2014. It continues to provide a platform for law enforcement and researchers across academia and the private sector to meet and exchange projects for training and research on cybercrime.
- **SOC, Security Operations Centre.** The SOC, which is headquartered in Lille, France, was created in 2018 as a private-public partnership in partnership with IBM. The Centre monitors the latest security threats and their impact as well as ensures that there is existing infrastructure to respond to these threats. [77] The SOC operates 24/7 and serves companies in France, ensuring data security for French enterprises and their foreign subsidiaries.

France also works bilaterally with various countries to develop their cybersecurity infrastructure. One initiative, which began in 2018, involves the development of an inter-ministerial partnership with Senegal to create a national school for cybersecurity in Dakar, Senegal. The School aims to enhance cyber security capacities across African States. As part of the Ministry for Europe and Foreign Affairs, France has provided funding for technical experts and specialised IT equipment, while assisting in the funding of regional vocational training programmes.[78] A similar initiative is ongoing in South Africa, with the French Embassy working with South Africa's Public Service Sector Education and Training Authority to increase cybercrime capacity building, by training approximately 350 forensic investigators on cyber forensic investigations. Training began in September 2017 (The Diplomatic Society 2017).

Financial Crime

The Financial Markets Authority (AMF) is France’s national agency for regulating its financial sector. In addition, France has special governmental agencies that are dedicated to countering illicit financial transactions pertaining to cybercrime.

- **TRACFIN, Unit for Intelligence Processing and Action against Illicit Financial Networks** (*Cellule Française de lutte contre le blanchiment de capitaux et le financement du terrorisme*). TRACFIN was established in 2007 to combat illegal financial transactions, money laundering, and terrorism financing. In 2018, TRACFIN created a new division dedicated to investigating financial cybercrimes. This investigative division aims to: i) develop its capacity to analyse publicly recorded blockchain transactions; ii) reinforce its links to Customs and with the C3N; and iii) develop international partnerships with other agencies countering cybercrime. TRACFIN identified multiple cybercrime threats facing the French nation, including increases in isolated Bitcoin purchases made by French businesses that were allegedly victims of ransomware attacks and increases in illicit products sold over the darknet (Ministere de l'action et des comptes publics 2019). In addition, TRACFIN highlighted that rapid increases in initial coin offerings (ICOs)[79] is opening up criminal opportunities for money laundering and fraud. TRACFIN has found that individuals rely on ICOs to launder their illicit funds, by purchasing tokens, which may then be sold to other investors before being converted into legal tender. In addition, entrepreneurs may use ICOs to scam investors, by offering fraudulent projects. Currently, France is attempting to establish a regulatory framework to help certify projects to reduce ICO frauds and regulate virtual currencies via the Business Growth and Transformation Action Plan (PACTE) bill, which was adopted by the French Parliament in April 2019.

France has developed a coherent infrastructure for building up its cybercrime capacities. Nonetheless, the country continues to improve these bodies and fill deficits in their digital security and protect information systems.

French International Bodies

In addition to state-level enforcement bodies that focus on cybercrime, there are also French international initiatives, which bring together law enforcement agencies and government bodies across French speaking nations. Two of these include the International Cybersecurity Forum and Francopol. The International Cybersecurity Forum is primarily interested in building bridges across the public-private sector, whereas Francopol brings together police agencies to enhance their capabilities and knowledge mobilization.

- **FIC, International Cybersecurity Forum** (*Forum International de la Cybersécurité*). The FIC is organised by the National Gendarmerie, and CEIS along with la Région Hauts-de-France. The main objective of FIC is to bring together various participants in cybersecurity, including security experts, lawyers, and digital players, to build bridges across the private public sectors and to bring together cybersecurity students and employers.
- **Francopol, International Francophone Police Training Network** (*Réseau international francophone de formation polici*è*re*). Francopol was established in 2008 by the Quebec provincial police agency, the Sûreté du Quebec, and the National Police of France with the aim of creating a francophone network where French law enforcement expertise could be shared among French-speaking nations.[80] Members of Francopol include law enforcement agencies in Belgium, Benin, Burkina Faso, Burundi, Cameroon, Canada, France, Luxembourg, Monaco, Spain, and Switzerland. Recently, Francopol has been involved in hosting international conferences focused on countering cybercrime.

Review of the French Cybercrime Literature

The French review resulted in the retention of 37 manuscripts, including peer-reviewed articles, government and public reports, book chapters, dissertations, and masters' theses. The literature retrieved from the French review was primarily characterised by theoretical and conceptual pieces that examined the different dimensions of cybercrime, including definitions and responses to countering it. Of the empirical pieces, the majority were exploratory and qualitative, providing in-depth analyses of specific cyber threats and/or offenders, with a select few drawing on quantitative analyses to assess effective means to deter cybercrime. In this review, we focus on the empirical studies to understand the nature of the threat; in addition, we use the conceptual and theoretical pieces to help contextualise these analyses.

Given the breadth of the search, we have organised the results into four main sections. The first section focuses on the ecosystem of cybercrime. This section comprises studies that have examined cybercrime as the collection of interactions between vendors and clients and how these relationships are initiated and maintained in order to carry out complex crimes. The second section focuses on the motivations of cyberoffenders, with a focus on studies developing typologies of hacker motivations. The third section details studies that have assessed the financial transactions of cyberoffenders and how they monetise their crimes. The fourth section outlines government and private sector responses to countering cybercrime. For each section, we provide a summary of the findings, identifying strengths along with areas that could be improved. Lastly, we conclude with future directions and identify gaps in our understanding of financial transaction systems and areas which cybercrime literature can move towards.

The Ecosystem of Cybercrime

Online environments support the convergence of enablers (e.g., coders and programmers of malicious software), vendors (e.g., sellers and traders of hacking tools and/or stolen data), buyers, and the targets of these attacks. The structure of these online networks can enable or constrain offenders' opportunities to commit cybercrimes. It follows, then, that any understanding of cybercrime requires an examination of the full set of actors across the online ecosystem. The francophone review identified many studies that mapped out the ecosystem of vendors, clients, and targets, with a focus on how offenders converge to commit their crimes. Together, these studies challenge many assumptions about how offenders collaborate within these ecosystems and carve out new insights on how offenders manage their online operations.

A major assumption of cybercrime is that the darknet provides an attractive platform for bringing together malicious actors to facilitate the initiation of online offences. Specifically, the anonymity of the darknet, coupled with the lack of geographic constraints, is theorised to foster the initiation and development of illegal activities. However, Dupont challenges this assumption in his detailed analysis of the operations of a major hacking network over a two-year period (Dupont 2016). His findings show that many of the features of the darknet that are viewed as promoting criminal opportunities (e.g., anonymity, lack of geographical barriers) are also responsible for breeding distrust and conflict among offenders, ultimately constraining the ability of illicit actors to operate efficiently.

In his study, Dupont conducts a detailed analysis of a major hacking network dismantled by a Quebec police agency in 2008 (Dupont 2016). The network consisted of ten men aged 17 to 25 who were arrested for infecting over 630,000 computers across 120 countries. The seized hard drives of the ten accused hackers revealed their private online conversations over the two-year period that the network operated. Analyses of these conversations showed that the group relied heavily on two leaders: one with the technical savvy who maintained the majority of the bots and served as a mentor for other group members and one with the social capital necessary to keep the group together. A content analysis of these conversations showed that the two leaders who appeared to complement one another – one with the social and the other with the technical skills – turned out to be the demise of the group. The relationship between the leaders rapidly deteriorated as the technical leader became frustrated with having to share his resources among his less competent collaborators. Further, the technical leader of the group – who had no problems coding the bots – was not well informed in even some of the most common bank frauds. Lacking social skills to establish and maintain co-offending relationships with others meant he was unable to keep the group together and convert the harvested data into sales. This case study of a group operating in Quebec, and likely French speaking, emphasized that interactions that took place online constrained the hackers' ability to build trusted relationships that are necessary to maintain durable co-offending networks.

A second major assumption of cybercrime is that reputation systems, similar to those offered by licit enterprises, such as Amazon, where peers can rank each other for services rendered, allow illicit markets to operate more efficiently. However, recent studies have suggested that these rating systems, designed to increase trust between offenders, are flawed. Using data from a hacking forum with over 8,000 members, Dupont showed that individuals rated other hackers primarily based on their personalities and/or to reciprocate the favour of a positive score, rather than provide an actual reflection of their criminal competence or hacking capabilities (Dupont 2016). Specifically, an analysis of the reputation scores on the forum showed that 86 percent of all evaluations between members were positive. A qualitative analysis of 25,000 randomly selected evaluations showed that 30 percent of all positive scores were for posting sarcastic or humorous content. The study showed that the majority of positive evaluations on the forum was guided not by technological competence or business acumen, but by an individual's social skill set and ability to deliver humorous content. As a result, reputation scores produced on the forum were not reliable indicators of hackers' competencies, creating challenges for individuals who may be seeking out suitable co-offenders online.

A third major assumption is that online environments provide an unlimited pool of suitable co-offenders. Online, offenders can theoretically access an unlimited number of potential co-offenders via illicit markets, forums, and chat rooms. Yet, recent studies have shown that these platforms have high levels of deception and fraud, with victimization often occurring among peers, thereby preventing the efficient functioning of these online systems. For instance, Décary-Hétu and Eudes' study, using data seized by the Swiss authorities, showed that there were high degrees of deception on a carding forum where offenders sold or purchased stolen financial data. Using forum data from over 75,000 members, the authors examined the extent to which users deceived other members by creating multiple user accounts – violating a golden rule of the forum – that each individual has a single username (Décary-Hétu and Mélanie 2015). The authors identified users with multiple accounts/usernames through three strategies: i) accounts that provided the same contact information, ii) accounts that used the same password (only passwords with a certain degree of complexity were considered), and iii) whether the moderator of the forum had previously flagged the user for having multiple accounts. Findings showed that nine percent of users on the forum had more than one account. In addition, the findings suggested that users were regularly victimised by their peers who sold information that they did not have or information that had expired, or by sending the same information to multiple vendors, all of which raise questions about the stability of these markets.

The challenges of finding suitable co-offenders and the level of deception in online environments suggest that the anonymity of the Internet – originally heralded as a hotbed for crime – may constrain the number and quality of available criminal opportunities. This is also supported by Bellido and colleagues who found that online markets present prime venues for the victimization of cyberoffenders (Bellido et 2017). Examining several websites known for selling false identity documents, the authors found that many of these websites were scams: selling fake products to users and exploiting clients for their money without providing them with the product. Because generating fake documents requires that the buyer provide personal identifying information (e.g., name, sex, date of birth, photograph), vendors had ample opportunity to exploit customers. Vendors may threaten to divulge this information if they receive complaints from customers, and customers may have little recourse for action.

However, while online forums may not be perfect for finding suitable co-offenders, others have found that online forums may still provide a valuable resource for individuals hoping to acquire cyberskills and competencies. Montégiani showed that hacking communities provide promising milieus in which to learn and pass on skills from more experienced to more rookie members (Montégiani 2017). Data for the study came from *hackforum*, a discussion forum with over 3.6 million members, with more than 55.5 million public messages. The study focused on a sub-forum, “Beginner Hacker”, over a one-month period, with 821 members and 3,636 messages. Analysis of the members active on this forum showed that there were a select few actors who were central within this community – posting multiple comments and serving as mentors for a large portion of the community. Rookies were often linked to multiple mentors simultaneously, allowing them to draw from the knowledge of multiple sources. A content analysis of these messages showed that the majority of the messages between members were positive, suggesting a supportive community where hackers were able to share and pass along information. Thus, forums may provide valuable resources for hackers wishing to develop or acquire new skills. However, the study did not detail the nature of this advice and whether it assisted in learning how to translate hacking activities into financial proceeds of crime.

Summary

The emergence of the darknet led many researchers and policymakers to theorise about how the online platform would increase the efficiency of the cybercrime ecosystem. The anonymity of the darknet decreases offenders’ risks of being detected by law enforcement agencies. However, studies in the francophone review highlighted that the anonymity afforded by this online platform increases offenders’ risks of being victimised by other offenders. The recourse mechanisms offenders can employ in traditional offline illicit markets to reduce the risk of deception and fraud, for instance the threat or use of violence by offenders engaged in illicit activities in offline contexts, are not available to online offenders. The lack of recourse mechanisms, coupled with the anonymity of the darknet, creates risks for users who wish to co-offend over these platforms. In addition, high levels of deception mean that online co-offending networks are susceptible to internal disruption. The prevalence of deception in online platforms, means that co-offending partners are often suspicious of one another, creating challenges for offenders to maintain attacks over extended periods. In addition, reputation systems on these forums, which are designed to increase trust by ‘vouching’ for hackers and providing validation of hackers’ criminal skills and competencies, are flawed. High reputation scores tend to be based on social charisma, such as humour, rather than technical aptitude or reliability, which are the skills that would make for an attractive co-offender. Together, these studies highlight the challenges faced by cyberoffenders on the darknet and how these challenges may make individuals less inclined to capitalise on the systems available on the darknet.

The extant francophone literature highlights how trust is created, maintained, and dissolved within the cybercrime ecosystem. Most of the French studies relied on digital trace data from online forums and private conversations to map out the social interactions among hackers with the aim of understanding how offenders converge and interact in online spaces to carry out cybercrimes. Digital trace data present a valuable resource for analysing the online ecosystem and provide information on the social interactions of offenders, the types of products sold, and the scope of crimes across the online environment. However, the data also present challenges for understanding the financial aspects of these ecosystems. For instance, researchers are limited in their ability to discern whether sales made in online markets represent scams aiming to victimise peers or reflect true products, taking product advertisements at face value. In addition, users' identities are masked behind usernames. Thus, there may be more than one individual behind a single user account, or a single individual may be behind multiple usernames. More apparently, digital trace data preclude us from understanding offline interactions. Individuals may converge in offline settings before moving to online environments, or vice versa. Together, this lack of understanding creates challenges for researchers wishing to study the flow of financial transactions across the illicit ecosystem and how offenders monetise their crimes.

Cyberoffender Motivations and Typologies

Cyberoffender motivations inform us why offenders commit their crimes and the types of targets they are more likely to attack, and provide insight into where funds are being sourced. The francophone review identified five studies that developed typologies of hacker motivations and targets. These studies drew on case studies of major hacking incidents (Décary-Hétu 2013), a crowdsourced dataset of DDOS attacks (de Mereuil et al. 2016), online attacks reported in news articles (Dupunt, Lavoie, and Fortin 2013), targets of botnet attacks (Freyssinet 2015), and hacking incidents perpetrated by jihadists (Ducol et al. 2018). Below, we detail these studies and their main findings.

Décary-Hétu provided a detailed analysis of the inner-workings of three major hacking incidents, broadly classifying their motivations into three categories: i) hackers motivated by profit, ii) hackers motivated by overcoming technical barriers, and iii) hackers motivated by ideology (Décary-Hétu 2013). The first case study highlighted a hacking network motivated by profit, involving four Romanians accused in 2011 for having remotely infiltrated the payment systems of 200 stores and restaurants by guessing or decrypting the passwords of these systems. Once accessed, the hackers had total access to the systems as well as the data stored on these systems, allowing them to copy the credit card numbers from every transaction. The hackers regularly transferred the data to external servers or onto other hacked computers, and then converted the information into profits by selling it to buyers who paid for the information via bank transfers from Western Union. After receiving payments, the hackers sent the stolen information to clients by email or by simply providing the client access to the server. In some cases, the hackers made a profit by using the credit cards themselves to purchase products online. In total, the operation stole information from over 80,000 credit cards.

In contrast, the second and third case studies represent hacking groups with non-financial motives. The second case study examined the hacking network of four individuals accused in 2010 for the creation of Wiseguys Tickets Inc. The network aimed to overcome regulations imposed by ticket markets, that limited the number of tickets that buyers could purchase for each event. The four members of Wiseguys Tickets lacked the technical competence to carry out the attack, and thus contracted with hackers to create a software capable of mimicking human behaviour, thereby allowing them to reserve tickets in a fraction of the time it would take a human being. Wiseguys Tickets set up shell companies to purchase IP blocks and rent servers to conduct the attacks (Zetter 2010).

In addition, Wiseguys Tickets relied on social engineering, registering with the same service that provided the CAPCHA code as the sites that sold the tickets. Having access to all the CAPCHA codes, as well as the source code that generated the CAPCHAs on these sites, allowed Wiseguys Tickets to program a robot to find the answers to the CAPCHA on the ticket website, thereby tricking the system into thinking they were legitimate buyers. Wiseguys Tickets took additional precautions, which included always using new IP addresses and new pseudonyms to create fake identities to access the website each time. Once acquired, the tickets were resold on a secondary market. This case illustrates how hackers require both technical competencies and social engineering skills to produce major attacks and how non-financially motivated hackers can cause major economic disruption. However, this case study did not provide information on how the hackers paid for their services.

The third case study highlighted the hacking network, Anonymous, that hacked a series of companies in retaliation for the censoring of Wikileaks in 2011. One of the targeted companies included HBGary Federal, an IT firm that offered security products and services to US organizations, such as the National Security Agency. The Anonymous group exploited a faulty configuration in the IT company’s website to access an encrypted list of the passwords of its administrators. Once downloaded, the hackers were able to obtain the decrypted passwords of leaders in the company and obtain full control of the company’s website.

Across the analyses, Décary-Hétu highlighted similarities and differences between the hackers' operations. Most of the hackers were young males (Décary-Hétu 2013). However, the hackers varied in their levels of education and their employment backgrounds. Further, while some operated in-house, bringing together individuals well-versed in hacking, others sourced out technical capabilities. Despite classifying the three networks into two main categories (profit versus non-profit motivations), there was no discussion on how the actors knew one another or how they disposed of their profits, thus providing limited information on the monetization process.

Other scholars have relied on crowdsourced datasets of DDOS attacks to create typologies of hacker motivations. De Mereuil & Bonnefous classified a dataset of 234 DDOS attacks reported to the website hackmageddone.com (n = 196) and in media articles on the database Factive (n = 38) into two broad categories: those motivated by profits and those not motivated by profits (de Mereuil 2016). Attacks motivated by profit represented 40 percent of all attacks. These hackers had a variety of targets and were involved primarily in taking possession of business websites for which they demanded ransom and harvesting stolen data. The authors classified attacks not motivated by profit into six additional categories: i) ethical hackers who aim to help their targets (e.g., to warn the target about faulty security in their operating systems), ii) libertarian hackers (e.g., groups such as Anonymous who aim to increase the freedom of expression), iii) trolls who conduct attacks for the pleasure of it, iv) cyber-jihadists who conduct attacks on behalf of extremist organizations, v) censors who conduct attacks to censor information they do not agree with, and vi) geopolitical hackers who use their hacks to intervene at the international level in geopolitical conflict, often directly attacking governments, such as the Israel Defense Team. Across these hacking groups, most attacks targeted the financial sector, including banks (83%), financial markets (11%), as well as sites for virtual currency transactions, such as Bitcoin (6%). The study showed how the financial sector was often targeted by hackers, regardless of whether motives were for-profit or not. However, the study provided little detail about the dataset and how attacks were classified into each of the categories.

In contrast to earlier studies, Dupont, Lavoie, and Fortin found that hacking attacks were primarily directed against social media sites (Dupont and Fortin. 2013). The authors identified 683 hacking incidents reported in news media articles over a 14-month period (October 2008 to December 2009). The study found that social media websites, including Craigslist, MySpace, Facebook and Twitter, were prime targets for hackers, stating that the large volume of non-verified content that circulates on these websites provides prime venues to bait users and infect computers. However, similar limitations to the ones confronted by DeMereuil and Bonnefous (2016) were also found in this study. Specifically, the sampling strategy of news articles may have misconstrued results, as infections on large platforms may plausibly be more likely to result in news coverage.

Focusing on botnets, Freyssinet relied on a crowdsourced dataset of 413 botnets reported to the French website, botnets.fr to classify attacks into different categories (Freyssinet 2015). He found that botnet attacks fell into one of 24 categories, ranging from click fraud to ransomware to Trojan attacks. The most common botnet attacks included ‘police locks’ (13%), which used a virus to block the victim’s computer while publishing an ad by a police agency, tax collector, or other fictitious agency, accusing the victim of having committed a crime or infraction. The attacker then demanded the victim pay a fine before the ad was removed; however, the study did not provide any information on the specific payment system used to pay this fine. The second most common category involved ‘*loaders*’ (12%), a borrowed English term used to describe botnets that provide the botnet master with the ability to remotely control the infected computer, or bots, and are often used for pay-per-install operations, and banking botnets (11%), which consisted of malware that collected online banking credentials or helped individuals take control of existing financial connections. The study highlighted the variety of botnet attacks, but also that hackers tended to rely on certain attack types, such as ‘police locks’, more than others.

Focusing on cyberjihadist incidents, Ducol and colleagues classified 169 hacking-related incidents made available by the International Institute for Counter-Terrorism from January 2013 to June 2016 into two broad categories: defensive and offensive actions (Ducol and Dupont 2018). Defensive actions included incidents where actors in jihadist movements supplied cybersecurity advice (e.g., forums dedicated to instructing jihadists on how to send anonymous messages, communicate using encrypted messaging services, and protect computers from spyware). Offensive actions were classified into two sub-categories: i) the defacing of websites, where jihadists would change the visual content to that of their own messages; and ii) the hacking of accounts. These hacking incidents primarily included collecting and then sharing personal data (e.g., doxing) on social media websites. A prime example of doxing involved the online jihadist forum Shumukh Al-Islam which published a list of 30,000 employees of the National Intelligence Agency of Israel on March 24, 2013, including their names, residential addresses, phone numbers, and email accounts. Similar attacks were perpetrated by the Islamic State Hacking Division, which created a public document containing the names and photographs of more than 100 employees of the US army. These cases, although limited, highlight how hacking does not only produce physical damages but can also lead to violent outcomes, such as the publishing of kill lists outlined above.

Summary

The literature on hacker motivations has primarily highlighted major categories of offenders (e.g., for profit and not for profit hackers). Individuals with financial motivations were found to have a high variety of targets and were more likely to select targets based on the popularity of the target to maximize gains (e.g., large sporting events). Across the studies, hackers motivated by financial profits tend to be classified together in a single group. In contrast, hackers not motivated by financial gain have been classified into multiple sub-groups: individuals with ideological motives, who hack to promote freedom of expression, to curb views opposite to their own, and those who wish to further an extremist cause (e.g., cyberjihadists). Most hacking attacks resulted in property damage or losses, regardless of whether the hackers were motivated by profit or not. However, attacks by cyberjihadists present a unique category, as these incidents were sometimes used to promote violence, with hackers stealing and publishing personal data (e.g., residential addresses and phone numbers) with a call to attack these individuals (i.e., 'kill lists'). Although these incidents represent a very small number of cases, they demonstrate how hacking can lead to both violence as well as financial losses.

Studies on hacker motivations has yet to examine how motives of for-profit hackers may vary across incidents. The extant literature on cybercrime motives and typologies tell us very little about the financial components of the crime. For instance, De Mereuil and Bonnefous classified nearly half of all DDOS attacks (40%) as financially motivated, but tell us little about how these attackers cash out or make profits (de Mereuil and Bonnefous 2016). More information on how hackers can be classified based on how they reap profits, the type of currencies they use, how they sell their data, and their success rates in ransom efforts would be valuable for understanding cyberoffences and designing intervention strategies. The study by Décary-Hétu offers some insight into these processes, finding that the hackers relied on Western Union transfers to receive payments and email to transfer the data (Décary-Hétu 2013). However, this study represents the exception among those cited, providing the only detailed analysis of the financial components of the crime although most incidents were classified as financially motivated.

Lastly, the studies highlight challenges of developing reliable and valid hacker typologies. There currently are no representative samples of hackers. Thus, what we know about hackers comes from convenience samples sourced from media reports, crowdsourced websites, and/or law enforcement investigations. In addition, motivations of hackers are inferred based on the sites they target. Thus, we may deduce that an attack was financially motivated if there was any potential for profit or the victim was a bank, but such deductions may not reflect the actual hackers' motivations. For instance, Décary-Hétu's study found that although one member of the hacking network reaped large profits, profit was not the initial motivation for conducting the hack Décary-Hétu 2013; D'Elia 2014). Often, we do not know the true motivations of cybercrime, whether it is sabotage, for espionage, or simply financial gain (D'Elia 2014).

Cryptomarkets

Most studies focused on English language cybercrime; however, there is a small literature that focuses on francophone experiences in cybercrime. The francophone literature on cybercrime also examined the structure of cryptomarkets, including the sale of false identity documents (Bellido et al. 2017), illicit drugs (Flamand 2018; Giannasi et al. 2012; Mireault et al. 2018; Paquet-Clouston et al. 2018; Rossy et al. 2018), and tobacco online (Décary-Hétu et al. 2017). These studies explore the scope of cryptomarkets, the number and volume of sales, and compare illicit online markets to their offline counterparts.

In the only francophone study to examine the sale of false identity documents online, Bellido and colleagues identify the scope of the illicit market (Belido et al. 2017). The authors develop a two-step strategy to identify the number of illicit markets selling false identity documents online. First, keyword searches on popular search engines were used to identify an initial set of sites selling these documents. Second, all the hyperlinks on each website were examined to obtain a final sample of 375 websites involved in the sale of forged documents. Most of the websites were located on the clearnet, particularly on video-sharing platforms, such as Dailymotion and YouTube (37%), as well as blogs and forums (27%). The authors found that forged documents were less commonly found on the darknet, accounting for only 19 percent of all identified websites. Most vendors preferred using email as their main method of contact with clients (86%); moreover, there were few unique vendors, with many vendors sharing the same email address. However, the type of email accounts most commonly used was not provided. The most common forged documents sold online were drivers’ licenses, followed by passports, and identity cards. The study also found that many of the websites were known for fraud, with several allegations that the websites were scams by other online users.

Other studies in our French language review examined the scope of drug markets, including the GBL market, a precursor of GHB, a synthetically produced sedative that is commonly used as a ‘date rape’ drug, and the untaxed tobacco market. A study by Giannasi and colleagues aimed to identify the number of websites selling GBL (Giannasi et al. 2012). The authors used targeted keyword searches across popular search engines to locate 39 websites involved in the sale of GBL from June to December 2011. The authors showed that most GBL websites were hosted in the Netherlands (80%) where the substance is not prohibited. An additional analysis examined the interconnectivity of the websites, using the sites’ logos, contact information, source codes, and IP addresses to identify which sites involved the same vendors. Results showed that 17 of the websites were controlled by six distinct groups, highlighting the interconnectivity of the online market, with many vendors relying on multiple sites to maximize sales of their products. Lastly, the authors examined longitudinal trends in GBL websites, finding that, over the sample period, while some of the websites disappeared (n = 4), many new ones emerged (n = 16). However, no information on the payment portals or transactions was provided.

Examining how vendors managed their online drug market operations, Rossy and colleagues relied on surveys of Swiss law enforcement agencies who described recent investigations (Rossy et al. 2018). Of the investigations, most were for clients who purchased drugs online for personal consumptions. However, the authors also detailed two investigations where vendors purchased drugs through online markets to resell locally. In the first case, the client would purchase drugs online (the nature of these transactions in terms of marketplace and purchasing strategies were not documented), and then have the drugs delivered to a mailbox in another country (in this case Germany) rented for this purpose, and then resell the product on the darknet to Swiss users. In the second case, the client also sent the purchased product to reception centres across different cities in Germany, employing people in charge of receiving the order. The merchandise was then resold in smaller quantities across other darknet markets, including Dream Market and Nucleus. All communications with clients were encrypted and all payments were made in Bitcoin, with the vendor having multiple Bitcoin accounts that regularly went through mixers, the exact ones not identified by the study, to attempt to eliminate their traceability.

Examining the scope of the online illicit tobacco market, Décary-Hétu and colleagues relied on a webcrawler to scrape all product advertisements found across 14 cryptomarkets on the darknet (Décary-Hétu et al. 2017). A total of 147,560 advertisements were scraped in the Fall of 2016. These ads were primarily found in the following cryptomarkets: AlphaBay (41%), DreamMarket (34%), Valhalla (12%), Applemarket (4%) and Darknet Heroes League (3%). Of these ads, only 476 were for illicit tobacco, representing less than 1 percent of all products advertised on cryptomarkets. Information on past purchases suggested that 6,304 USD of tobacco products were sold across these 14 markets over a 30-day period in the Fall of 2016. The UK was identified as one of the main source countries, accounting for one quarter of the total revenue for illicit tobacco products. Vendors who sold tobacco products also tended to sell other drug products (49% of vendors), potentially due to the relatively low sales of illicit tobacco.

The relatively small size of the online tobacco market raises questions about the degree to which the sale of drugs on online platforms reflect sales made offline. Mireault and colleagues aimed to answer this question by comparing online and offline drug sales made in Canada (Mireault et al. 2018). The authors compared online and offline drug sales by drawing from various data sources. For online drug sales, they examined drug advertisements on the darknet across vendors in eight cryptomarkets that identified Canada as the country of origin. For offline drug sales, they relied on seizure data, surveys of drug users, and toxicological analysis of used water samples. Findings showed that cannabis was the most common drug observed across both online and offline sales of drug markets. However, online drug markets tended to sell a much higher rate of stimulants, including MDMA/Ecstasy, LSD, cocaine, and methamphetamine, as observed in the offline data sources. The study suggests that online markets may attract a different type of vendors, as well as clients, who may source different drugs online than they do in offline markets. However, differences across markets may also be attributed to transport of drugs: stimulants are much easier to ship, given their compact size as compared to more easily detectable drugs, such as cannabis.

Also comparing online and offline drug markets, Flamand examined whether vendors who sell drugs online are also involved in offline sales (Flamand 2018). The author used surveys of cryptomarket vendors which asked about their drug market activity, including whether they sold drugs offline, the types of drugs they sold, and the total value of drugs they sold. A total of 133 vendors responded to the surveys, with 57 vendors completing or nearly completing the full survey. Of these 57 vendors, 46 percent reported selling drugs in offline, traditional markets as well as on cryptomarkets. Comparing vendors who sold drugs only in online markets to those who sold drugs in both online and offline markets showed that the latter group was more successful financially, making higher profits overall. In addition, this group was found to sell similar types of drugs on cryptomarkets and in the offline world while being more likely to source drugs offline. The results of this study emphasize that many vendors who operate online migrated from offline drug markets, and that they were able to capitalize on their offline experience, increasing their overall profits and ability to source illicit product. In addition, the study also showed that, while some vendors transition from selling drugs in offline to online markets, the onset into selling drugs for other vendors began online. Understanding how these offenders initially began their onset into drug selling may be important for developing effective interdictions to deter offenders before they start; this study did not survey, however, how offenders acquire the startup capital and skills necessary to engage in their criminal activities.

Other studies in the francophone review focused on how cryptomarket vendors manage their online profiles. Analysing over 183,391 messages posted to the Silk Road 1 discussion forum, comprising of 39,367 participants, 708 of which were vendors, Paquet-Clouston and colleagues found that drug vendors use these forums as platforms to advertise their products (self-promotion), putting links to their websites or promoting the quality of their products, as well as to provide advice to others (e.g., how to properly consume drugs (Paquet-Clouston et al. 2018). Similar to the hacking forum, interactions among participants were primarily positive, with individuals using the forum mainly to thank others for their business or advice. Negative interactions tended to come from individuals who were in more senior positions who had higher reputations. Overall, the study highlighted that discussion forums were used by vendors to extend their roles as entrepreneurs as well as to serve as ‘voluntary’ experts on drugs. From this perspective, forums served as an extension of the online markets, a place to advertise one’s products as well as secure one’s status as an expert, potentially serving to secure reputation and further sales.

Most studies of cryptomarkets focus on English or Russian language cryptomarkets; however, a report authored by the IT security company, Trend Micro, provided a unique focus on French Underground markets. According to the report, the French underground is distinct from traditional English language markets that tailor to individuals in North America. First, the report outlined that French underground markets were more challenging to access, with many online platforms providing additional vetting processes to filter out non-native French speakers and law enforcement. Platforms often required a vetting process, such as obtaining a reputation prior to posting or accessing the website. Second, the report argued that the French underground is better equipped to prevent users from being scammed by other users, by having a more prevalent use of ‘shame walls’ where individuals can publicly report the usernames of individuals who have been dishonest or scammed them in the past. However, these ‘shamed’ users may easily evade detection or repercussions, by switching their usernames with relative ease, and thus their online identity, prior to committing another fraud. Thus, the effectiveness of this shaming is largely unknown, but it may decrease the length during which a single user may perpetuate a fraudulent scam. Third, French underground markets tend to be small in scope, catering to a niche French-speaking clientele, offering fake receipts and bank account information for financial firms in France; French personal identification, such as drivers’ licenses; and weapons that are illegal within the country’s borders. The study provided insight into how markets may adopt different practices across various languages; however, it did not provide a methodology of the markets and/or forums surveyed or how the authors reached their conclusions.

The study also suggested that opportunities for fraud and victimization may be differentially distributed across markets. As compared to non-French language markets, the report suggested that French language markets actively compete with one another. To support this perspective, the report discussed instances where the administrators of French marketplaces often capitalised on their positions to victimise vendors who were also active in other markets. If two vendors sold their products on more than one French market, the administrator of one market would attempt to use the other vendor’s credentials to hack into the other’s account with the goal of stealing funds and closing the account.

Summary

Cryptomarkets represent a small portion of the overall illicit market. Despite their relatively small scale, cryptomarkets provide important platforms for understanding how illicit wares are sourced, distributed, and sold online. Online markets, enabled by access to a network connection, have left digital trace data that have opened the door for a new wave of criminological studies. Much of what we know about illicit markets online comes from studies using data from online markets across the darknet and clearnet. For instance, researchers have used webcrawlers to scrape drug ads across illicit markets or have used targeted keyword searches across popular search engines to identify the number of sites selling illicit products online.

Only a fraction of the studies reviewed relied on traditional data sources (e.g., self-reports and official records) to support their findings. Official data, such as arrest records, have been suggested to be a poor indicator of cybercrime, given low levels of reporting to police and relatively few law enforcement interdictions. However, while official records may provide poor indicators of cyber-activities, self-report data may represent an important and under-exploited source for examining cybercrime payment systems and for supplementing the findings from digital trace data. Digital trace data provide information about the product advertised online (e.g., product descriptions and vendor reputation), but often provide little information about the vendors themselves or insight into how vendors conduct their financial transactions. Self-report data have been used extensively to understand financial transactions and offender income in offline illicit markets but are scarcely used to understand vendors in online illicit markets. This represents an important omission, given that the anonymity afforded by the darknet provides researchers with ample opportunity to directly reach out to illicit vendors online and survey them in an anonymous environment about their activities.

Studies from the French review emphasized that online markets are not independent of offline markets. Similar products are sold in both online and offline settings, potentially creating additional market competition. Furthermore, vendors often sit on both online and offline markets, selling their wares on both online forums as well as in-person, to maximize their sales. How online markets impact offline sales and how vendors bridge these two markets have important implications for disrupting these markets. These studies raise additional questions about how interdictions may displace sales from one market into another. For instance, individuals who have experience in offline markets may displace their online sales in favour of offline ones – or vice versa – in response to interdictions, thus, making it essential to understand financial transaction systems in both online and offline settings and how vendors manage their illicit incomes across both platforms.

Proceeds of Cybercrime

The French review identified a select few studies that focused on the financial transaction systems of cyberoffenders. Here, we first outline the findings from studies that describe how hackers profit from their crimes (Paquet-Clouston et al. 2018; Dupont and Benoît 2014; Décary-Hétu and Mathieu 2018; Auer & Stijn 2018; Pernet 2016; Dupont 2014). We then turn to a select few studies that have used novel approaches to understand how cyberoffenders use virtual currencies (Décary-Hétu and

Lavoie 2018) and how government interventions can impact the value of these currencies (Auer and Clasens 2018). Lastly, we examine the types of financial transaction systems used in French underground markets (Pernet 2016).

Providing an overview of the different stages of carrying out a botnet attack, Dupont highlights the various points in the process where botnet masters may profit from their activities (Dupont 2014).[81] The study highlighted how financial transactions happen at two different points in the botnet supply chain: *traders* may sell or rent out the botnets and/or purchase additional software to continue propagating the botnet while *monetizers* have the skills or criminal contacts to convert the stolen data into revenue or launder the acquired money. There is no indication of which financial systems are used for these transactions or how the proceeds are cashed out or laundered.

The creation of a botnet begins with the creation of a malware that extracts relevant information (e.g., documents, emails, or passwords) and cannot be detected by infected machines. However, the process of creating a successful botnet does not stop there. Botnet masters run the additional challenge of maximizing the number of machines they infect. They may do this in a number of different ways, including running phishing campaigns, putting the malware on legitimate Internet websites that are not well-protected, or they may hire brokers to install the application on their machines, remunerating the individual(s) based on the number of infections they deploy and the geographic distribution of the contaminated users. This represents the first potential point of profit for individuals involved in botnet schemes. The second potential point for profit is in exploitation – extracting the financial data for profit – or the neutralization of the victim (e.g., click-fraud, emptying bank accounts, or reselling information on forums) (Allaire 2015).

A recent study by Majdalany provided evidence of specialization among a sample of experienced botmasters. Drawing from all conversations on the ‘introduction’ subsection of the Darkode forum – an invite-only hacking forum classified by the FBI as one of the biggest global threats to digital infrastructure – the study classified the 88 individuals who posted into one of seven roles: *coders* (programmed and wrote the code for the botnets), *traders* (sold, rent, or bought botnets), *distributors* (propagated botnets and distributed malicious software), *operators* (operated the network, and command and control centres), monetizers (monetized the botnets), the *curious* (indicated an interest in botnets), and the *experienced* (indicated prior experience with botnets, but did not detail their roles). Of these 88 individuals, the vast majority fell into a single role (83%). Less than a fifth (17%) of the individuals, reported being involved in multiple roles. Coders were the main group to occupy multiple roles, with the most of these coders also specializing in the distribution of botnets. In addition, the study also showed that even among one of the largest hacking forums very few individuals mentioned having any competencies in the monetization of botnets, with only 22 percent of the 88 individuals reporting experience as *traders,* selling or renting out the botnets, and even fewer reporting involvement in their monetizations (3%). However, the study provided little detail on how these individuals monetized botnets, the payment systems they used, or transactions that were made.

Décary-Hétu and Lavoie present one of the few studies to examine the use of virtual currencies by cyberoffenders (Décary-Hétu and Lavoie 2017). The authors provide a novel attempt to uncover how virtual currency is being used by online offenders by examining the use of Bitcoin wallets by malicious actors. First, the authors developed an open source tool, BitCluster (available at http://dev.bit-cluster.com), which assembled all transactions made by each Bitcoin wallet. The authors then obtained a list of 30 wallet identifiers that received ransom payments following a malware infection. The authors then used the *BitCluster* tool to download a list of all payments that each wallet identifier received related to the ransomware. They then conducted a descriptive analysis of the money accumulated within each wallet to determine the evolution of payments. They found that individuals involved in receiving ransom payments could be classified into three profiles. The first profile consisted of the least sophisticated ransom hackers, who used a single wallet to receive multiple payments over extended periods. For instance, one wallet was active over 58 days and received payments from 1,127 victims, approximately 10,000 USD per day, with the hackers making no efforts to camouflage their activities. The second profile comprised slightly more sophisticated hackers, stopping payments to their wallet within a few days. And the third profile comprised hackers who used a wallet only once to receive a single payment – before theoretically switching to another wallet – in an attempt to make it more challenging to follow their profits over time.

A final study by Auer and Claessens on the financial transactions of cyberoffenders shifts the discussion from how offenders rely on virtual currencies to monetize their crimes to how law enforcement interventions may influence the value of cryptocurrencies (Auer & Claessens 2018). The study used a dataset of 151 regulatory announcements, pertaining to cryptomarkets announced on Reuters from 2015 to 2018, to examine whether the volume (number of Bitcoin addresses) and value of various cryptocurrencies changed before and after the regulation announcement. The study focused on seven different cryptocurrencies (i.e., Bitcoin, Ethereum, Bitcoin cash, Litecoin, Monero, Zcash, Ripple (XRP)) and found that measures designed to target these cryptocurrencies devalued them. As an anecdotal example, the authors highlighted how in June 2018 a Japanese government agency requested that six cryptocurrency trading platforms improve their procedures to prevent money laundering. Shortly after this request, the value of the currencies plummeted. The study represents an important contribution for understanding cybercrime. Traditionally, cryptocurrencies have been viewed as independent from regulations. However, these analyses demonstrate that the value, volume, and who uses cryptocurrencies are highly sensitive to regulatory changes. The study's findings raise additional questions regarding how offenders manage their online illicit businesses, given that profits are made in a currency that may fluctuate in response to interdictions. Thus, it is important to understand how efforts to regulate cryptocurrency may in turn influence how offenders weigh the costs and benefits of using these currencies.

A report by the IT security company, Trend Micro, highlighted that payment systems may be distinct across French- and non-French language markets (Pernet 2016). In reviewing the French underground, the authors found that financial transactions on the darknet were made through Bitcoin and prepaid card services. Prepaid card services provide an anonymous payment solution for vendors and clients who may not wish to undergo the complexity of setting up a Bitcoin wallet. In France, individuals may purchase prepaid cards at many retail locations and are required to provide only a working mobile phone number to make the purchase. Thus, prepaid cards provide alternative payment that are less complex than virtual currencies, such as Bitcoin, but may afford similar security for making online transactions. In addition, certain markets in the French underground relied on escrow systems for making transactions. However, unlike other marketplaces, including ones tailored to German and Russian speaking audiences, some French marketplace escrow systems limited total transactions to 1,000 Euros. This means that every time vendors reach this amount, they have to wait until all their transactions are processed before they can engage in other transactions. Thus, restrictions imposed by French marketplace administrators may constrain the volume of illicit products sold.

Summary

Studies on the proceeds of cybercrime show that hackers primarily make profits as *traders,* renting out the botnet equipment, or as *monetizers,* converting stolen data into profits and laundering the proceeds of the crime. However, we know little about how these individuals are recruited into these operations and/or how they manage the proceeds of crime. Many studies highlighted the challenges hackers face to convert stolen data into profits. But few provided empirical examinations of how hackers have profited from their crimes, including the types of currencies they use, the amount they make, and how money is funnelled through the supply chain. Much of what we know about the ‘cashing out’ process of cybercrime in the French literature is from tangential or anecdotal cases. One of the few studies to focus on payment systems showed that the French underground is distinct from other non-French speaking marketplaces. This French underground typically relied on two types of payment systems: Bitcoin and prepaid card services. In addition, limits were often imposed on the maximum amount of Escrow, meaning that payments may be delayed.

Following illicit payment systems is a challenging endeavour in any setting but becomes particularly so in online markets where offenders may use cryptocurrencies over anonymous platforms. The anonymity of many virtual currencies, coupled with the fact that each person can have an unlimited number of wallets (for instance, one person could generate a million new wallets each hour), makes tracing the flow of money challenging, especially when one person may use a different wallet for each single transaction.

Despite these challenges, scholars have used innovative methods to understand how offenders use virtual currencies. For instance, Décary-Hétu and Lavoie developed an online tool to retroactively examine the number and volume of payments an offender receives via Bitcoin (Décary-Hétu & Lavoie 2017). However, this tool can only be used once the offenders’ wallet identifier(s) is/are known. In future analyses, the authors suggest that the tool may be used to help de-anonymize transactions by linking wallets to the same user based on similar purchasing profiles, potentially creating an avenue for understanding the flow of money through virtual currencies.

Other potentially promising avenues are partnerships with government agencies that monitor the flow of fiat- to virtual-currencies. For instance, in Quebec, enterprises that operate Bitcoin ATMs, where virtual currency may be transferred to fiat, and vice versa, are required to record transactions and provide these details to the Financial Authority. This information may be valuable to researchers who wish to understand the flow of transactions between the two systems. The importance of understanding how virtual currencies respond to governmental regulations to interdict these payment systems could be studied using this data. Previous researchers have shown that law enforcement disruptions can influence the value of Bitcoin (Auer & Claessens 2018). This has important secondary effects, given that offenders may see their potential profits increase or decrease, making some crimes more or less attractive, while contributing to users’ scepticism about the stability of the currency (Bodurov 2016).

The review highlights important gaps in understanding the proceeds of cybercrime. The lack of studies on this subject is primarily due to the lack of data sources on illicit financial transactions. One important gap in this literature, in particular, is the extent to which cyberoffenders rely on virtual currencies. Anecdotal evidence suggests that the complexity in setting up wallets may lead some offenders to rely on traditional forms of payment (e.g., fiat-currencies) for illicit transactions (e.g., Bellido et al., 2015; Bodurov, 2016; Décary-Hétu, 2013), despite the increased risk of disclosing their identities. Thus, virtual currencies are not always the preferred method of making purchases, with the complexity of setting up wallets leading some to use personal credit cards or other tenders to make purchases, indicating that researchers also need to pay heed to both systems for understanding cybercrime. The relatively small scope of these currencies puts into question the scale of money laundering. More information about what leads one offender and not another to use virtual currencies may help inform policies aimed to disrupt illicit transactions within these systems.

Responses to Cybercrime

The growth of cybercrime has led to parallel increases by policymakers, the private sector, and academics on measures to counter it. The francophone literature details current responses to combating cybercrime (Dupont 2014; Rossy et al. 2018), including the global infrastructure to combat cybercrime (Baumard 2013; D’Eilia 2014; Dupont 2016; Hathaway et al. 2015), and the effectiveness of strategies to disrupt cybercrimes (Allaire 2015; Calvet 2015).

Dupont classifies current approaches to combatting botnets into two categories: judiciarization, which consists of identifying, neutralizing, and punishing high-profile hackers (e.g., arrests and dismantling their command and control structure); and public-private partnerships between government and Internet Service Providers (Dupont 2014). He argues that judiciarization provides a limited strategy for tackling botnets because they are highly resilient to interdictions and can quickly recover from the removal of a single or limited set of actors. For instance, in the case of BredoLab, one of the largest recorded botnets, the attackers were able to restart their phishing activities using servers based in Russia only two days after their servers were seized by law enforcement. The redundancies in command and control servers mean that the survival of one can ensure the survival of the entire botnet. In addition, the sentences for perpetrators of botnets, which result from these interdictions, are typically short, with the arrested individuals often representing a low recidivism risk, tending to be first time offenders, with no violent histories, and high likelihoods of successful social integration.

In contrast, Dupont argues that partnerships between government agencies and Internet Service Providers (ISPs) represent effective measures to minimize threats posed by Botnets. ISPs play an important role within the digital ecosystem, having a virtual monopoly over the circulation of data that go through their network. The entirety of communications between infected computers and botmasters are transmitted through ISPs infrastructure, with a recent study finding that half of all spam diffused globally came from compromised computers relying on the Internet provided by 50 large ISPs. Thus, ISPs can play key roles in designing interventions and blocking illicit activities. Partnerships between government agencies and ISPs have already led to the creation of successful anti-botnet programs in Australia, Germany, Holland, South Korea, and the United States. These partnerships have relied on ISPs to create aggregated records of malicious flows to generate lists of currently infected computers. This list serves to inform each ISP participant of the IP addresses belonging to their clients where activity looks suspect. The ISP informs clients of the probable infection on their machines and provides tools to help clients get rid of the botnets along with free antivirus products. The updated list of infected computers allows ISPs to identify which users are incapable, delay, or refuse to correct the situation (e.g., in Japan, only 29 percent of clients corrected the situation). The government may also step in and restrict these users Internet access until they remove the infection from their computers These partnerships have been shown to significantly reduce the impact of botnets while being complementary to ongoing investigations by police agencies.

Despite the promise of forming partnerships between government agencies and ISPs to reduce the impact of botnets, Dupont highlighted that this approach has its limits. Botnets often operate across multiple jurisdictions, and thus the impact of partnerships with ISPs depends on transnational agreements for countries to effectively navigate and respond to threats that cross borders. For instance, the BlackShades botnet consisted of a network of computers that infected nearly half a million machines across ten countries. Its takedown led to 1,000 arrests across 16 countries in May 2014, requiring major international cooperation. However, difficulty in harmonizing national legislation and police responses across countries means that these interdictions are often challenging to implement.

To examine the existing global infrastructure to counter cybercrime, Dupont identified existing international cybercrime initiatives and the countries which belong to each initiative (Dupont 2015). Using data from publicly available sources, Dupont identified 657 organizations involved in 41 international initiatives to counter cybercrime. These organizations included private businesses (47%), nation-states (31%), NGOs and professional organization (16%), and international organizations (6%), such as Interpol. He then examined which organizations belonged to the same initiatives to understand how countries collaborate in the fight against cybercrime. The study was able to identify the countries with the greatest cooperation in international initiatives as well as nation-states that tended to be on the periphery, not entering into agreements with other countries. Findings showed that the United Kingdom was central to international cybercrime infrastructure, belonging to 49 percent of the initiatives, followed by Italy (43%), Canada (41%), France (41%), and the USA (41%). Dupont explained the UK’s central position by its high degree of cooperation with Commonwealth countries, including Australia, Canada, and New Zealand, as well as by belonging to many of the same agreements as the United States. The study also identified the private sector as key players in countering cybercrime internationally, with Microsoft serving as a broker between many of the private and public organizations. The study highlighted the need to examine the structure of international cyber regulation to understand how countries may respond to threats that cross national borders.

Baumard provides explanations for why nation-states may not elect to engage with international cybercrime regulations (Baumard 2013). Specifically, he identified two main challenges for countries that enter international cybercrime regulations. The first challenge for nations collaborating internationally is assigning responsibility, as it is not always clear which actor should be held responsible for cyberattacks. For some countries, it may be the person who created the bot, for others, it may be the state that allowed the bot to operate in the country. The second challenge for nations cooperating across borders is sharing instances of cybervictimization with other states. States are risk-averse to sharing vulnerabilities in their defence system, which can provide insight into their cyberinfrastructure, and the sophistication of their defence capabilities. Building on this, D’Elia offers additional challenges for creating international agreements, with cybercrime creating ambiguities that may cause conflict between nation states (D’Ellia 2014). Countries see cyberspace as a sovereign domain that only they should have control over, and often do not know who is behind cyberattacks, meaning that nation states may interpret an attack by a private actor as a state being behind it, raising potential for additional conflict. D’Elia suggests that academia and Centres of Excellence are in better positions to bring about international frameworks and share research findings internationally as to how best to respond to cybercrime. Yet, the capabilities of academia to mobilize knowledge about cybercrime and enhance international cooperation requires that these researchers are familiar with current responses to cybercrime, something that is rarely reported by countries (Hathaway et al 2015).

A study by Allaire examined the relative effectiveness of current laws and policies on disrupting botnets (Allaire 2015). Specifically, he examined whether policies that aim to counter cybercrime, anti-spam laws, public private partnerships with ISPs, and law enforcement interdictions had any impact on the actual number of reported malware infections. Data for the study came from a major antivirus software company, ESET, who controlled eight percent of the market globally at the time of the study. Every time a threat was detected by the software it was reported to ESET, providing a valuable data source for understanding the scope of botnets. Identifying ten countries who adopted at least one of the three policies, Allaire examined the number of reported malware cases two years before and one year after the adoption of the policy. Findings showed that governments that adopted public-private partnerships with ISPs were the most effective at reducing the number of malware cases, whereas anti-spam laws had no effect, and law enforcement interdictions had an effect but only when they targeted multiple actors and servers in the network. The study was exploratory in nature, only providing bivariate statistics to compare the number of detected malware incidents before and after the implementation of the policy, meaning that the study did not allow for causal inference. However, the study confirmed Dupont’s suggestion that private-public partnerships were the most effective strategy for disrupting botnets; the number of detected malware cases in a country dropped after governments developed partnerships with private companies to counter cybercrime. The study highlighted the promise of secondary data obtained from private security companies as an important resource for evaluating the effectiveness of cybercrime policies (Dupont 2014).

Another study by Calvet took a different approach to examine the effectiveness of disruption strategies (Calvet 2013). The author reproduced a botnet network, *Waledac,* which at the time of its operation had more than 390,000 machines under its control, in a laboratory environment and then deployed various interdictions to see how effective they were at disrupting the botnet’s operations. *Waledac* first appeared on the Internet in November 2008 and was notable for its propagation method. Initially, it was propagated through social engineering by convincing users through emails to download the program and execute it (e.g., Christmas cards and the announcement of Barack Obama's resignation). But in 2009 the operators of the botnet created a new means for propagating it by generating a remuneration infrastructure which paid individuals based on the number of times they were able to infect other machines; no information, however, on how specific payments were made was provided. This strategy accounted for 98 percent of the propagation network and allowed the operators to make money from infected machines by sending spam on behalf of other groups, stealing email addresses, obtaining passwords, and conducting DDOS attacks. In the laboratory environment, the study varied the number of repeaters directly targeted (e.g., 5, 10, 100 and 250 repeaters targeted) to examine how the number of targets impacted the botnet's operation, measured as the number of servers that remained under the botnet's control, the processor load, and the number of emails received each minute. Findings from the study showed that even targeting a small number of bots had an impact on disrupting the majority of the network.

The relative ineffectiveness of law enforcement approaches to countering cybercrime was further highlighted by Rossy and colleagues (Rossy et al. 2018). The authors surveyed 23 Swiss law enforcement agencies to understand how they investigated cybermarket offences. The surveys asked the agencies about the number of investigations they had conducted on the darknet, along with details about the three most important investigations linked to the sale of online drugs in the past four years. Of the 23 police services, only 39 percent (n = 9) indicated investigating cases of online drug sales, across both the clearnet and darknet. These investigations were primarily for cannabis products, followed by synthetic drugs (e.g., ecstasy, methamphetamine, LSD). Law enforcement agencies reported primarily conducting an investigation after a product was intercepted by customs. These postal investigations showed that most online drug sales were for personal consumption rather than resell. Most online orders were sourced from darknet markets (e.g., AlphaBay, Hansa), but websites on the clearnet were also important sources for drugs (e.g., cemb.eu, shayanashop.com), with law enforcement finding that drug sales took place on a variety of websites, including dating sites. Although many personal users used Bitcoin to purchase products, other users were found to use their personal credit cards, since Bitcoin represented too complicated of a process for many clients (a finding consistent with Bodurov's (2016) survey of Bitcoin users).

Summary

The extant francophone literature highlights the role of public-private partnerships in countering cybercrime. Law enforcement responses may be ill-equipped, primarily responding to high profile instances, or only able to interdict a select few actors involved in an international scheme. In contrast, partnerships with Internet Service Providers provide a means to survey the online landscape to identify suspicious activity and victims of botnets. This top-down approach aims to reduce the impact of botnets by identifying those affected and providing them with the necessary tools to reduce their victimization. The importance of public-private partnerships in reducing the threat of botnets was first advanced by Dupont (2014) and then formally tested by Allaire who showed that countries who adopted these partnerships had fewer malware attacks.

The francophone review also points to the importance of academic partnerships with the private sector in order to secure data that can further our understanding of cybercrime. For instance, Allaire was able to assess the effectiveness of countering cybercrime policies across countries, thanks to a partnership with an international IT security company, which provided information on the number of malware infections within each nation-state it was operating (Allaire 2015). However, few studies examined disrupting the financial transaction systems in their investigations. Responses were primarily aimed at reducing the impact of attacks that had already been generated rather than developing preventative measures.

Conclusion

Technological shifts have enabled new forms of offending and anonymization for offenders to converge and commit crimes on online platforms. The francophone literature outlines the breadth of cyber offences and scope of monetization techniques. However, the review also challenges many of the assumptions about the role the Internet plays in enabling these offences, highlighting the difficulties in locating suitable co-offenders, particularly individuals well versed in the monetization process. Individuals proficient in monetization were scarce in hacking forums, suggesting potential challenges for offenders seeking out skilled partnerships (Majdalany 2017). Further, individuals seeking co-offenders were often victimised on forums, being scammed by their criminal partners, suggesting high levels of fraud and deception and issues of trust (Bellido et al. 2017; Décary-Hétu and Eudes 2015). Moreover, although financial motives were identified as primary considerations for offenders conducting cybercrimes, few studies detailed the financial transaction systems used to monetize crimes or the actors involved in these transactions.

The review also highlighted that despite the security afforded by virtual currencies, offenders often opted for less secure but more efficient financial transaction systems.

Offenders reported selling stolen data and malware using public payment systems (Décary-Hétu 2013), including credit cards (Bodurov 2016) and pre-paid card services (Pernet 2016; Décary-Hétu & Lavoie 2017; Rossy et al 2018). The complexity of setting up wallets, along with scepticism in the stability of virtual currency markets, and the challenges in transferring funds provides cues as to why some offenders opt out of these systems for illicit purchases (Bodurov 2016).

However, other studies emphasised the role of virtual currencies in illicit activities, including ransomware (Décary-Hétu and Lavoie 2017) and the sale of drugs in cryptomarkets (Rossy et al. 2018). But most of these studies did not detail how payments or transactions were made, or they were based on anecdotal cases, precluding the generalizability of these results. Furthermore, offenders also varied in how they used virtual currencies. While some offenders relied on a single wallet for all their illicit transactions, others used different wallets for each illicit transaction, maximizing their security (Décary-Hétu and Lavoie 2017).

In summary, the extant francophone literature lacks detailed studies on the precise mechanisms whereby cyberoffenders use currencies to cash out from crimes. One of the main challenges towards developing this body of research is the availability and reliability of data sources. The collection of reliable statistics on cybercrime lags behind other forms of crime. Traditionally, there have been two main sources to estimate the scope of crimes: official sources and self-report data. However, both suffer from issues when applied to cybercrime offences. Most cybercrimes are never declared to the police (Dupont 2013; Dupont 2014). Victims often do not know they were targets of a cybercrime incident, and, when they do know, they often fail to report it to officials. For instance, the private sector may prefer to handle the instance themselves rather than involve law enforcement agencies. Thus, law enforcement data is often restricted to a rare few cases. Self-report data is also flawed. Currently, self-reports of cybercrime victimization are not common practice and not standardised across countries. The UK represents one of the few countries to modernise digital risk statistics to include self-reports of cybercrime victimizations (Dupont 2014).

Because of the limits of self-report and official sources, the private sector has become a privileged source of statistics for digital risk assessments. The private sector, such as IT companies, record information on the number of viruses or malware detected, whereas Internet Service Providers (ISPs) can monitor the flow of information for botnets and compromised computers. However, a reliance on these numbers also creates its own challenges. The private sector faces competing pressures, including marketing and sensationalism to promote its products, so while it may make the risks more tangible the risks are often misrepresented (Dupont 2014). Further, the private sector does not provide standardised methodologies across data collection. When reported, statistics are often incomplete, biased, and disparate, making them unusable. However, this does not stop government agencies from using them (Côté 2016; Gómez 2014), creating additional concern about how assessments of cybercrime risks are generated (Prates et al. 2013). Despite these challenges, previous studies highlight that the private sector provides an important point of contact for moving research forward, offering insight into the scope of attacks thereby allowing us to assess the effectiveness of disruption strategies and to trace the flow of cyberattacks (Allaire 2015).

In no other area is the lack of data more apparent than when it comes to understanding cybercrime and financial transactions. What we know about financial transactions is often inferred through anecdotal case studies, which rarely detail the full process from the initiation of the act to the cashing out. One potential avenue is the use of public information on Bitcoin transactions. This information is publicly available, and tools have been developed to quickly aggregate all transactions made by each wallet (Décary-Hétu and Lavoie 2017). However, the ability to link wallets across users creates challenges which makes these sources difficult to rely on. We often do not know how many actors are behind each wallet, or how many wallets each actor has. To move forward requires sourcing new data.

Currently, much of our knowledge of cybercrime comes from two primary data sources: digital trace data (e.g., Bitcoin transaction data, market information, and forums), and official sources (e.g., secondary analysis of law enforcement investigations). Although official sources are limited (only a fraction of crimes are reported to the police), the use of self-reports and surveys may present a promising avenue forward to improve our understanding of online payment systems. The anonymity of the darknet affords immense opportunities for talking directly to pools of cyberoffenders. Although this approach is not without its caveats (e.g., confirming they are actual offenders and reliability of responses), it opens up new opportunities for data collection. Only one study in the review used survey data to understand cyberoffences. This study also represents one of the few studies that addressed where offenders source their income (e.g., across online and offline markets) (Flamand 2018). The darknet provides a means to distribute surveys to large numbers of individuals (e.g., individuals selling illicit wares also provide contact information), while also ensuring their anonymity (e.g., administering the survey over secure and protected platforms). In the criminology literature, much of what we know about payment systems comes from surveys and interviews with offenders. There is also reason to believe that this presents a promising way to move forward our understanding of online crimes.

Works Cited

ANSSI, L'Agence nationale de la sécurité des systèmes d'information. 2018. *Rapport Annuel.* (France: l'Agence nationale de la sécurité des systèmes d'information (ANSSI), 2018).

Allaire, Marie-Renée. 2015. *Lutte Aux Botnets: Les Politiques De Prévention S' Avèrent-Elles Efficaces?.* Masters, Université de Montréal.

Auer, Raphael, and Stijn Claessens. 2018. *Réglementation Des Cryptomonnaies: Évaluation Des Réactions Du Marché.* BIS.https://www.bis.org/publ/qtrpdf/r_qt1809f_fr.pdf.

Baumard, Philippe.2013. "La Régulation Des Contre-Mesures Contre Les Cyber Attaques." *Archives de philosophie du droit* 57: 177-95.

Bellido, Lena, Simon Baechler, and Quentin Rossy. 2017. "La Vente De Faux Documents D'identité Sur Internet." *Revue internationale de criminologie et de police technique et scientifique* 70, no. 2: 233-49.

Bodurov, Ivelin. 2016. *Les Transferts De Fonds Virtuels–Une Technologie Innovatrice Et Un Moyen Potentiel De Blanchiment D'argent*. Masters, Université de Montréal.

Calvet, Joan. 2013. "Analyse Dynamique De Logiciels Malveillants." PhD., École Polytechnique de Montréal.

Côté, Anne-Marie, Maxime Bérubé, and Benoit Dupont.2016. "Statistiques Et Menaces Numériques: Comment Les Organisations De Sécurité Quantifient La Cybercriminalité." *La Découverte* 3, no. 197-198: 203-24.

D'Elia, Danilo. "La Guerre Économique À L'ère Du Cyberespace. 2014." *Hérodote* 1-2, no. 152-153: 240-60.

de Mereuil, Albert, and Annabel-Mauve Bonnefous. 2016. "Anatomie D'une Cyber-Attaque Contre Une Entreprise: Comprendre Et Prévenir Les Attaques Par Déni De Service." *Gérer et Comprendre*: 5-14.

Décary-Hétu, David. 2013. “Cybercriminalité: Entre Inconduite Et Crime Organisé. Edited by Francis Fortin’’. In *Piratage Informatique.* Québec: Presses internationales Polytechnique et Sûreté du Québec.

Décary-Hétu, David, and Mélanie Eudes. 2015. "Partenariats Criminels Au Sein D’un Forum De Carding: Alliés, Rivaux Ou Escrocs? Étude De L’utilisation D’identités Virtuelles Multiples’." *Revue internationale de criminologie et de police technique scientifique* 68, no. 3: 299-314.

Décary-Hétu, David, and Mathieu Lavoie. n.d. Bitcluster: Un Outil D’analyse des Bitcoins.

Décary-Hétu, David, Vincent Mousseau, and Ikrame Rguioui. 2017.*Le Trafic Illicite De Tabac Sur Les Cryptomarchés.* Université de Montréal.

Ducol, Benjamin, Maxime Bérubé, and Benoit Dupont. 2018. "Le Piratage Informatique, Nouveau Répertoire D'action des Mouvements Contestaires Violents?". In *Délinquance Et Innovation*, edited by David Décary-Hétu and Maxime Bérubé. Montreal, Quebec: Les Presses de l'Université de Montréal.

Dupont, Benoît. 2013. "La Coévolution De La Technologie Et De La Délinquance: Quelques Intuitions Criminologiques." *International Annals of Criminology* 51, no. 1-2: 39-56.

Dupont, Benoît . 2014. "

Dupont, Benoît. 2014. "La Régulation Du Cybercrime Comme Alternative À La Judiciarisation: Le Cas Des Botnets." *Criminologie* 47, no. 2: 179-201.

Dupont, Benoît.2016. "Les Liens Faibles Du Crime En Ligne: Écologie De La Méfiance Au Sein De Deux Communautés De Hackers Malveillants." 3, no. 1: 109-36.

Dupont, Benoît, Pierre-Éric Lavoie, and Francis Fortin. 2013. ‘’Cybercriminalité: Entre Inconduite Et Crime Organisé.’’ In *Crimes Sur Le Web 2.0*. Edited by Francis Fortin. Québec: Presses internationales Polytechnique et Sûreté du Québec.

Flamand, Claudia. 2018. *Vente De Drogues Illicites Sur Le Darknet: Enchâssement Des Marchés De Drogues Physiques Et Virtuels*. Masters, Université de Montréal.

Freyssinet, Éric. "Lutte Contre Les Botnets: Analyse Et Stratégie." PhD, Université Pierre et Marie Curie, 2015.

Giannasi, Pauline, Diego Pazos, Pierre Esseiva, and Quentin Rossy. 2012. "Détection Et Analyse Des Sites De Vente De Gbl Sur Internet: Perspectives En Matière De Renseignement Criminel." *Revue Internationale de Criminologie et de Police Technique et Scientifique* 65, no. 4: 468-79.

Gómez, Rodrigo Nieto. "Cybergéopolitique: De L'utilité Des Cybermenaces. 2014." *Hérodote* 1, no. 152-153: 98-122.

Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri. 2015. *Indice De Préparation À La Lutte Contre La Cyber-Criminalité - Version 2.0.* Arlington, VA: Potomac Institute for Policy Studies.

Majdalany, Chloé. 2017. *Les Botmasters Et Leurs Rôles Dans Le Marché Des Botnets*. Masters, Université de Montréal.

Ministere de l'action et des comptes publics. 2019. *Tendances Et Analyse Des Risques De Blanchiment De Capitaux Et De Financement Du Terrorisme En 2017-2018.* Traintement du renseignement et action contre les circuits financiers clandestins. *France*. TRACFIN.

Mireault, Caroline, Vincent Ouellette, David Décary-Hétu, Frank Crispino, Pierre Esseiva, and Julian Broséus. 2018. "Le Trafic De Drogues Illicites Sur Le Darknet: Un Reflect Du Marché Traditionnel?". In *Délinquance Et Innovation*, edited by David Décary-Hétu and Maxime Bérubé. Montreal, Quebec: Presses de l'Université de Montréal.

Montégiani, Caroline. 2017. *L'apprentissage Social Chez Les Pirates Informatiques: Analyse De L'influence Des Relations D'entraide Et De Conflit Sur Le Processus D'apprentissage*. Masters, Université de Montréal.

Paris Call for Trust and Security in Cyberspace. 2018. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Paquet-Clouston, Masarah, Cateline Autixier, and David Décary-Hétu. "Comprendre Les Interactions Des Vendeurs De Drogues Illicites Sur Les Forums De Discussion Des Cryptomarchés. 2018." *Canadian Journal of Criminology and Criminal Justice* 60, no. 4: 455-77.

Pernet, Cedric. 2016. ”The French Underground: Under a Shroud of Extreme Caution*.” Trend Micro*. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-french-underground-under-a-shroud-of-extreme-caution.

Prates, Fernanda, Frédérick Gaudreau, and Benoît Dupont. 2013. "La Cybercriminalité: État Des Lieux Et Perspectives D'avenir." In *Droits De La Personne: La Circulation Des Idées, Des Personnes Et Des Biens Et Capitaux*, edited by Institut canadien d'études juridiques supérieures, 415-42. Cowansville, Quebec: Éditions Yvon Blais.

Premier Ministre. 2015. *French National Digital Security Strategy.* Secretariat-General for National Defence and Security. France: Secretariat-General for National Defence and Security.

Reitano, Tuesday, Troels Oerting, and Marcena Hunter. 2015. "Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce." *The European Review of Organised Crime* 2, no. 2: 142-54.

Rossy, Quentin, Ludovic Staehli, Damien Rhumorbarbe, Pierre Esseiva, Frank Zobel, and Larissa J Mayer. 2018. *Drogues Sur Internet: Etat Des Lieux Sur La Situation En Suisse.* Lausanne.

The Diplomatic Society. 2017. "France and South Africa Tackle Cyber Crime." *The Diplomatic Society*. https://www.thediplomaticsociety.com/archive/archive/2202-france-and-south-africa-tackle-cybercrime.

Discussion: What We Learned about Transactions in Cybercriminal Contexts

Our assessment of the extant literature on transactions in criminal contexts reveals a number of key outcomes as well as a host of new questions that will need to be anticipated and addressed moving forward. Ultimately, it is important to recognise that studying cybercrime must be a reflection of the ways in which it is conceived, regulated, and responded to not only in international contexts but also in domestic contexts. With this in mind, we built the current assessment around two guiding questions regarding the *modus operandi* of cyber offenders engaging business models and the manner in which public and private entities respond to their offending within the context of political, jurisdictional, and financial limitations inherent within each of the five geographical locations we identified for this report.

A key determinant of the strategies and capabilities of various criminal actors in this space is whether they are based in developed of developing countries. Primarily, this manifested itself in two ways, which were calibrated to the competencies of offenders and the capabilities of prevention professionals (e.g., law enforcement). This include the sophistication of systems and infrastructure to support common offending activities (e.g., more sophisticated and technologically savvy offenders engaging in more complex forms of fraud or online theft among developed country offenders vs developing country offenders, and in response to similarly differentiated capabilities of the home country's law enforcement). This also includes a differential focus on types of crime engaged in.

Offenders from developed countries are more likely to be the ones who commit more sophisticated forms of crime because they have access to the technology to do so and also because they must contend with similarly sophisticated prevention and interdiction capabilities of the law enforcement agencies based in their country. These higher standards demand more sophisticated skillsets. Accordingly, there are fewer high-tech offenders with greater capabilities compared to the overarching offender pool which would encompass low-tech offenders as well. Additionally, FinTech infrastructure is highly concentrated in developed countries (particularly in the US in Atlanta and the UK in London), making them a target for sophisticated hacks and fraud attempts. Payments processing companies in these countries are critical components of the online financial transaction ecology and their status as corporate entities adds a layer of complexity to implementing strategies to prevent financial crime, particularly when there is a lack of cooperation between private and public entities.

Developing countries completely lack such industries or maintain them at relatively unsophisticated levels and thus do not have to contend with developing similarly sophisticated investigation and enforcement strategies. It is important to maintain an understanding of the role of old technologies in cybercrime and current research does not appear to keep pace with the expansion of digital uptake and market penetration in emerging markets, which may cause ongoing failures to accurately characterize the shifting cybercrime scene in these spaces, both in terms of technological knowledge and access and domestic political and capacity considerations. Currently, the level of sophistication and array of software and communications platforms available to those in developing countries, as well as the ability and will of law enforcement authorities in such countries is significantly less sophisticated. As such, most financial offenses perpetrated by offenders in a developing country are simpler and based on the ability to magnify offending attempts through a combination of democratised online platforms

(Facebook, WhatsApp, PayPal) and the application of simple yet effective social engineering techniques that can be distributed to hundreds of individuals to convince them to part with their money (via deception and fraud) rather than by taking it (via online theft or hacking). Present limitations in terms of higher-tech offender opportunity in these developing markets are not likely to remain the case; increased access to technology, particularly technology that is dated and with old, unpatchable operating systems equates to a large attack surface for potential criminal actors.

Recognising these shifts in offending profiles and offender opportunities underscores the need to not only understand the behaviours of individuals who use the digital environment to facilitate criminal offending but also how the financial infrastructure influences these offences. Accordingly, as the usability of media and communications platforms (particularly social media) increases, we anticipate a significant increase in social engineering-based fraud to occur with concomitant responses to these attempts by the owners of these platforms in both developed and developing countries. As security and deterrent measures are enabled on such platforms (e.g., two factor authentication, facial recognition, etc.), these kinds of offenders will simply migrate to other platforms with similarly high usability potentials and popularity to replicate their efforts with a new group of victims. These efforts will be abetted by the tendency of software and communications companies to roll out their products before properly hardening them against such efforts in their attempt to beat the competition to market.

The greater emphasis for those in law enforcement in such ecologies will be on secondary prevention – identifying, and recuperating losses – rather than on primary prevention measures to “crime-proof” an ever-expanding pool of technologically unsophisticated vulnerable victims. Moreover, better identifying attackers’ based on how they reap profits, the type of currencies they use, how they sell their data, and their success rates in ransom efforts would be valuable for understanding cyberoffences and designing intervention strategies, such as making it more challenging for offenders to find trustworthy co-offenders, which could better constrain the number and quality of available criminal opportunities.

Differences in attack opportunities between developed and developing countries means that the size and amount of funds transferred or lost in the commission of crime cyber-related crimes are greater per offender in developed countries compared to developing countries. In developed countries, like the UK, the US, Australia, and, to some extent Russia and China, fewer, more sophisticated offenders had access to more powerful, complex financial platforms, allowing them to take full advantage of cryptocurrencies, blockchain technology, dark web exchanges, IoT, and unsanctioned payments systems. In developing countries, more and more offenders are able to take advantage of the usability of common social media and communications platforms to target larger populations of potential victims who are otherwise unsophisticated in their knowledge of criminal activity.

Consequently, a bifurcation of crime prevention strategies is afoot. More high-level investigation and intervention systems and agencies in developed countries will focus their attention on the most sophisticated actors capable of enacting the highest impact offenses, ignoring many lower level offenders. Attention to sophisticated actors is exemplified by FATF’s guidance to adopt regulatory standards regarding cryptocurrency-related businesses, in an effort to prevent money laundering and terror finance. However, compliance is variable and uneven, with developing countries often struggling to institute effective and/or transparent oversight mechanisms, which could result in a balloon effect of some mobile cyberoffenders moving to countries or using products with weaker oversight. The ignoring of low-level offenders is exemplified with the industry standard response to credit card fraud. Most credit card agencies do not wish to expend thousands of dollars per offense to pursue low level fraud and hacking that results in hundreds of dollars of loss. They calculate such losses into their shrinkage estimates and pay insurance to handle the rest. This response has clear implications for offenders who are able to scale their small-scale offending; aggregated small-scale attacks will likely generate sufficient revenue to continue offending with little risk of capture, given current response frameworks.

To that end, those perpetrating online crime in developing countries have fewer and simpler options (which are mostly a subset of those also available in developed countries plus others, such as certain payment systems unique to certain developing countries) to perpetrate their offenses. But the greater numbers of offenders and the democratization of communications and payments technologies – including cryptocurrencies, sanctioned alternative and unsanctioned alternative payments systems, and especially the proliferation, anonymity, and usability of mobile banking platforms – means that while they are able to process less funds per capita the overall effect (in terms of losses) is similar.

A knock-on effect of this bifurcation is that the development of agencies designed to combat cybercrime will be widely different depending on the level of resources provided and sophistication of enforcement required by different governments. This asymmetry in capabilities makes cooperation and coordination difficult even for governments and private entities that want to work together. The addition of differential enforcement priorities further exacerbates the problem and will make it easier for offenders to commit their crimes given their lack of concern for jurisdictional boundaries. Finally, the sophistication of financial platforms – both sanctioned and non-sanctioned – adds an additional layer of complexity to prevention and interdiction efforts, especially when such platforms are bolstered by strong encryption and anonymization (e.g., blockchain technology, AI, etc) and have the ability to foster liquidity across different types of payment formats. These challenges will require greater collaboration between governments, but as importantly, greater collaboration across different sectors, including private companies, academic and research institutions, as well as governments. Such collaboration should be focused not only on enforcement and intervention but data sharing, open-source code, and "just-in-time" research, to allow for nimble and nuanced responses to threats as they arise, and that begins to investigate the latter half of the economic cybercrime script, the disposal of the proceeds of financial crimes, of which there is currently little knowledge.

We suggest three key areas for future research: criminal opportunity, regulatory responses, and law enforcement responses, in diverse financial ecosystems; the disposal of the proceeds of cybercrime; and, criminal opportunity and victimisation in regional settings, particularly in the developing world.

First, it is important to develop research agendas that recognise the relative importance of different financial ecosystems to offending strategies and patterns. Cryptocurrencies have generated a lot of scholarly and regulatory interest. It is clear that increases regulatory coverage throughout the world has reduced the value of cryptocurrency as a potential large-scale value vehicle for cybercriminals; in other words, cryptocurrency becomes less valuable to offenders the more difficult it is to cashout without oversight. Accordingly, continued research on how virtual currencies and other innovative transaction methods respond to governmental regulations, and appear or disappear in criminal activity, should continue to be supported. However, we contend that digital fiat currencies represent the most important financial ecosystem vis-à-vis cybercrime, and keeping up to date with non-traditional transaction systems such as mobile money, QR code transfers, and prepaid cards is increasingly important, and must be prioritised in future research. Moreover, there is a danger in under-playing the importance of these technologies and the modest tools that facilitate their transfer, such as smartphones.

Second, there is little research that focuses on the disposal of the proceeds of cybercrime. Part of this is due to access problems, compounded by a reluctance and lack of patience to fund the digital and analogue ethnographic or offender-based research that could elucidate this knowledge gap. Some spaces will be difficult to study, such as state-sponsored economic cybercrime; however, lower-level actors should be able to be studied and researchers must be supported to develop innovative methodologies to do so.

Finally, future directions of research need to not forget regional and developing cybercriminal concerns. Regional technologies often spread to other places, so understanding, for instance, user vulnerabilities and offenders' opportunities to leverage these new payment technologies will help harden those technologies as they gain wider traction. Moreover, it is critical to remember new users of the internet. The majority of new users of the internet will be from developing nations, and internet penetration across the world is projected to increase sharply. A large array of potential problems needs to be considered. Some examples include: how new users understand risk and risky situations online; how using old, out-dated technologies, that new users are more likely to have access to impacts risk; how the introduction and uptake of emerging payment systems which increasingly are replacing cash transactions in the developing world, create criminal opportunities and public vulnerabilities. Ultimately, these systems will not remain local – they will span diasporas and the world economy – and supporting efforts to reduce the risks associated with their usage will contribute to a healthier cyberspace for all users.

Footnotes

1. In 'legality principle' jurisdictions such as Germany and Italy, for example, formal discretion not to enforce is not permitted and prosecution is required when there is sufficient evidence. So strategic thinking needs to take a different shape. ↩
2. Though the Netherlands, to give one example, fluctuates in the criteria by which it criminalizes self-laundering. ↩
3. There is a case in India's Supreme Court that has been rescheduled several times with the latest date reported October 15th, 2019. It was not heard then either. ↩
4. In 2017, the US Department of Justice ordered Western Union to pay USD $586 million to settle fraud charges. Between 2004 and 2005, Western Union received

over 550,000 complaints about fraudulent transfers. Most of these reports related to cybercrimes (McGuire 2018). ↩

5. Anonymity is an element that early cryptocurrency adopters cherished. While there are privacy focused cryptocurrencies, there has been an increase in regulatory efforts on exchanges, which focus on identifying funds and the people who they belong to, at the cashing out process. Though unregulated exchanges persist (Gandal et al. 2018), an increasing proportion of exchanges are accepting regulation as a cost of continuing to do business, particularly in Western economies. ↩
6. Other E-gold-type transmitters exist, such as C-gold, based in the Seychelles; however, C-gold requires strict identity verification to open an account (White 2014); C-gold does not appear in the cybercrime literature nor commonly as a payment option in DarkWeb marketplaces. ↩
7. Although cryptocurrencies were not mentioned explicitly in any compliance reviews, the FATF placed Panama on its 'grey list' in 2019, noting "Panama will work to implement its action plan, including by: (1) strengthening its understanding of the national and sectoral ML/TF risk and informing findings to its national policies to mitigated the identified risks; (2) proactively taking action to identify unlicensed money remitters, applying a risk-based approach to supervision of the DNFBP sector…; (3); ensuring adequate verification and update of beneficial ownership information by obliged entities, establishing an effective mechanisms to monitor the activities of offshore entities, assessing the existing risks of misuse of legal persons and arrangements to define and implement specific measures to prevent the misuse of nominee shareholders and directors, and ensuring timely access to adequate and accurate beneficial ownership information; and (4) ensuring effective use of FIU products for ML investigations…and continuing to focus on ML investigations in relation to high-risk areas…." (FATF 2019). Item (3) above may be applicable to PerfectMoney and similar bodies. It is not known whether PerfectMoney cooperates with criminal investigations locally or internationally. ↩
8. WebMoney was first registered in 2018. At the time of writing, its status was still active (see: https://web.archive.org/web/20191107145733/https://register.fca.org.uk/ShPo_FirmDetailsPage?id=001b000000m4IXoAAM). ↩
9. The Council of Europe's Budapest Convention on Cybercrime does not provide for a monitoring-mechanism. In 2013, however, the Council of Europe T-CY started to

carry out assessments regarding the implementation of the Convention by the Parties, based on questionnaires. These are open to all signatories world-wide, whether or not they are members of the Council of Europe. There is no formal output or outcome assessment of this review process, and it is likely that major effort goes into capacity-building and legal frameworks rather than the effect it has on crime, as is the case for money laundering evaluations that are done more intensively and are mandated (Levi et al., 2018; Levi, 2020). ↩

[10] https://web.archive.org/web/20191107203751/http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html. ↩

[11]
Ransomware:
http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=fc4481a5ea80 11.88 EUR;
http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=a15d0668ca31 1.99 EUR;
http://rufr2d2l6i5j4vsj.onion/product/7076/126/29266 $6.50;
http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=29dc089246c7 16.28 EUR

Exploit kits:
http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=00782d2db6c7 1 EUR;
http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=7862110dfd67 8.75 EUR;

Malware: http://rufr2d2l6i5j4vsj.onion/product/8491/126/16883 $44.45 ↩

[12] http://crackerbuplauso3.onion/en/hacking-services/services.php $600 ↩

[13] See: http://2x4tmsirlqvqmwdz.onion/#/ssn for example. ↩

[14] See: http://2x4tmsirlqvqmwdz.onion/#/dedicated $4-$19;
http://rufr2d2l6i5j4vsj.onion/product/22365/131/85220 $14.99;
http://rufr2d2l6i5j4vsj.onion/product/25668/131/36031 $12;
http://rufr2d2l6i5j4vsj.onion/product/19427/131/78240 $1.22;
http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=a2f9caa02411 $29.99. ↩

[15] See: http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=d8e1fc759a5e 2.2 EUR; http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=7616710ae5a5; http://vn5socks.net/ $3/65/15 $100/200/365; http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=1d8965c70fa0 $2 / 2 EUR; http://rufr2d2l6i5j4vsj.onion/product/67333/133/191028; http://vip72.com/ $20; http://rufr2d2l6i5j4vsj.onion/product/40247/129/100770 $19.99 ↩

[16] See: http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=2950ca0ae430 3.55 EUR; http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=b6768ad357ad 3.81 EU; http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=b267ade45935 1.71 EUR; http://5vp364htrfrx2v2fg3q4miz673opdee256meup2e46dpt3524lwhxsid.onion/index.php?c=listings&a=product&code=34e368300688 5.99 EUR; http://rufr2d2l6i5j4vsj.onion/product/6932/132/16883 $5.56; http://rufr2d2l6i5j4vsj.onion/product/37584/132/186763 $1.99; http://rufr2d2l6i5j4vsj.onion/product/42789/132/191028 $4.99. ↩

[17] https://www.scmp.com/news/china/society/article/2189065/warnings-issued-after-britain-freezes-chinese-students-bank; https://www.universityworldnews.com/post.php?story=20190307200521986. See more generally, https://www.cifas.org.uk/newsroom/new-data-reveals-stark-increase-young-people-acting-money-mules; *https://www.europol.europa.eu/newsroom/news/over-1500-money-mules-identified-in-worldwide-money-laundering-sting*; https://www.bbc.co.uk/news/uk-england-45797603 (all accessed 15 December 2019). See also NCA reviews of Chinese underground banking: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/445-chinese-underground-banking/file. ↩

[18] Bisq is an open-source, peer-to-peer application that allows someone to buy and sell cryptocurrencies in exchange for national currencies. No registration is required. It is found at https://bisk.network. ↩

19. Atomic swaps, or atomic cross-chain trading, is the exchange of one cryptocurrency for another cryptocurrency, without the need to trust a third-party. ↩
20. CoinJoin is a trustless method for combining multiple Bitcoin payments from multiple spenders into a single transaction to make it more difficult for outside parties to determine which spender paid which recipient or recipients. Unlike many other privacy solutions, CoinJoin transactions do not require a modification to the Bitcoin protocol. ↩
21. elibrary.ru ↩
22. https://www.msu.ru/ ↩
23. https://www.hse.ru/ ↩
24. https://carnegie.ru/ ↩
25. https://www.imemo.ru/ ↩
26. www.arett.ru ↩
27. https://en.mvd.ru/ ↩
28. Russia’s Federal Security Service. http://www.fsb.ru/ ↩
29.

Russia’s Federal Service for Supervision of Communications, Information Technology and Mass Media.

https://rkn.gov.ru/ ↩

30.

Russia’s Ministry of Digital Development, Communications and Mass Media.

https://digital.gov.ru/en/ ↩

31.

Russia’s largest provider of digital and telecommunication services.

https://www.company.rt.ru/en/about/ ↩

32.

Russia’s biggest state-owned banking and financial services company.

https://www.sberbank.ru/↩

33. http://www.consultant.ru ↩
34. https://www.kommersant.ru/theme/1267 ↩
35. https://www.group-ib.com/ ↩
36. https://rt-solar.ru/products/jsoc/ ↩
37. https://www.ptsecurity.com/ru-ru/ ↩
38. https://jet.su/ ↩
39. https://www.kaspersky.ru/ ↩
40. https://qrator.net/ru/ ↩
41. Currency exchange (RUB to USD) that we present throughout this review is up-to-date as of summer 2019. As exchange rates change, we advise to prioritise reported data in rubles, as the USD equivalent may change. ↩
42. The Commonwealth of Independent States is a regional intergovernmental organisation of 12 post-Soviet republics in Eurasia formed following the dissolution of the Soviet Union. Those countries are Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan. ↩
43. The Shanghai Cooperation Organisation (SCO) is a Eurasian political, economic, and security alliance, established by the Shanghai Cooperation Organisation Charter in 2002. It includes China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan as full members and Afghanistan, Belarus, Iran, and Mongolia as observer states. ↩
44. Chapter 28 of the Russian Criminal Code titled “Crime in the field of computer information” contains articles 272, 273, 274 and 274.1. These articles cover the issues of illegal access to computer information, malware, misuse of computer information and effects on critical infrastructure. ↩
45. An example is the Cobalt group whose chief operator was arrested in March 2018 in Alicante, Spain. With malware attacks, the group targeted over 100 financial

institutions, banks, and e-payment systems in more than 40 countries. The gang began their activity in 2013, and their criminal operations resulted in cumulative losses of over 1 billion EUR for the financial industry. The criminals used malware of their own design, known as Carbanak and Cobalt (Europol 2018). Despite the arrest of the operator, Cobalt appeared to be active in the following months where the attacks mainly focused on banks in Russia and CIS countries. However, based on the content of the spear phishing email, it is likely that western financial organisations were also targeted (Group-IB 2018b). It is speculated that the Cobalt group consists of over 100 people (BI.ZONE 2019). ↩

46. While there is no official data on the exact number of cases, it is reasonable to suggest that many victims do not report small-scale theft from their cards. As Goryacheva and Trifonov (2019) reported for *Kommersant*, in Moscow only 20 to 30 clients of the major banks in Moscow reported theft from their bank cards to the police in the first half of 2019, while some 100 additional clients of Binbank whose personal data was leaked online for sale filed police reports. These numbers do not correspond with the actual rate of this type of theft. ↩

47. For example, the Cobalt hacker group targeted banks, payment systems, and IT companies – constantly changing regions of interest. After a series of 'international' attacks, they focused on the CIS countries but later continued their attacks with no geographical patterns (Group-IB 2017). ↩

48. The Central Federal District is one of the eight federal districts of Russia. With almost 40 million people, it is the largest district by population. The district's largest cities include Moscow, Voronezh, Yaroslavl, Ryazan, Lipetsk, Tula, and Kursk. ↩

49. Overall, Bank of Russia (2019) reported that there were 21 known ATM incidents in 2018. The regulator also observed a decrease in losses from this type of attack: 12 million rubles (180,500 USD) in 2018 vs 40 million (601,600 USD) in 2017. ↩

50. SMS-banking is a form of mobile banking which enables clients to use SMS messaging to request account balance statements and perform simple financial transactions, such as transfers between the user's own accounts or electronic bill payments (for example topping up a mobile phone account balance). If the phone has been infected with malware, criminals can intercept SMS-messages and perform transactions on their own. ↩

51. For example, the author of TinyNuke banking PC trojan that attacked users in the United States and France has made the source code of the programme and its control system publicly available. Other malicious programmes with open source codes are an Android banking trojan Maza-in, the RATAttack toolkit, that uses the Telegram protocol, and the Mirai Botnet to undertake DDoS attacks (Group-IB 2017). ↩
52. For example, a Russian journalist willingly revealed an SMS-code (part of the 2FA) to criminals pretending to be bank employees on the phone. They used the information to steal 10,000 rubles (152 USD) from the journalist’s bank card (Kamaletdinov 2019). The journalist later explained that he was in a hurry and did not think much about the phone call at the time. ↩
53. Specialists associated the WannaCry attacks with the pro-government North Korean Lazarus group, while the NotPetya attack was attributed to the BlackEnergy group, most likely Russian (Group-IB 2017). ↩
54. VK is the most popular social media service in Russia. ↩
55. A distributed denial-of-service attack is a malicious attempt to disrupt normal traffic of a targeted server or network by overwhelming the target or its infrastructure with a flood of internet traffic. ↩
56. Other malware includes spyware, remote control malware, trojan-downloader, encryption malware, malware for deleting files, and banking trojans. ↩
57. https://money.yandex.ru/page?id=529405 ↩
58. https://www.webmoney.ru/rus/information/statistic/index.shtml ↩
59. https://corp.qiwi.com/company.action ↩
60. Silence is an APT type group that first targeted banks in Russia and later expanded its operations to CIS and Eastern Europe, specifically, Ukraine, Belarus, Azerbaijan, Kazakhstan, and Poland. In 2019, Silence once again increased the geography of its attacks, and in 2019, its presence has been detected in more than 30 countries. From June 2016 to June 2019, the group has stolen at least 4.2 million USD (Group-IB 2019). ↩
61. United Card Services (UCS) is the largest independent processing company in Russia, servicing about 20% of the transaction volume generated by the cardholders

of international and local payment systems in Russia. The company provides issuing and acquiring services for the cards of VISA International, MasterCard Worldwide, China UnionPay, JCB International, American Express, and «Mir» - a Russian payment system, as well as for merchants' local non-bank cards. ↩

[62] In the period from January to August. ↩

[63] https://money.yandex.ru/doc.xml?id=524780 ↩

[64] https://qiwi.com/settings/identification ↩

[65] This is an accordance with the Russian Federal Law No 115 on AML/FT. ↩

[66] https://www.webmoney.ru/rus/help/start/registration.shtml ↩

[67] In a survey conducted by PwC (2018), 22% of Russian respondents said that they had spent from two to more than 10 times as much on the resultant investigation as the losses from the crime itself; 15% said that they had spent the same amount on investigating fraud as they had lost. ↩

[68] Art 1, Regulations Governing the Establishment of the National Information and Communication Security Task Force. ↩

[69] In 2017, Decree No. 577 creates the Cybersecurity Committee in the orbit of the Ministry of Modernization, which is comprised of representatives of the aforementioned Ministry, the Ministry of Defense and the Ministry of Security. The objective of the Cybersecurity Committee is to clarify the National Cybersecurity Strategy. In addition to developing the National Cybersecurity Strategy, in coordination with the competent areas of the National Public Administration, the Cyber Security Committee is tasked with developing an action plan for the implementation of the National Cybersecurity Strategy (Presidencia de la Nación 2019). ↩

[70] According to Reyes Neira (2015), the category of more than USD $100 million is relatively small, representing approximately 30 organizations worldwide. ↩

[71] Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-

legitimate purposes), in contravention of national laws or, where applicable, international obligations (FATF 2010). ↩

72. A full list of these reports and publications can be found at https://www.ssi.gouv.fr/agence/rayonnement-scientifique/publications-scientifiques/articles-ouvrages-actes/ (Accessed August 5, 2019). ↩

73. See https://www.cert.ssi.gouv.fr/a-propos/ (Accessed July 29, 2019). ↩

74. See https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-cybercriminalite (Accessed July 29, 2019). ↩

75. https://www.gendarmerie.interieur.gouv.fr/pjgn/SCRCGN/Le-centre-de-lutte-contre-les-criminalites-numeriques-C3N (Accessed August 5, 2019). ↩

76. https://www.prefecturedepolice.interieur.gouv.fr/Nous-connaitre/Services-et-missions/Missions-de-police/La-direction-regionale-de-la-police-judiciaire/La-brigade-d-enquetes-sur-les-fraudes-aux-technologies-de-l-information (Accessed July 29, 2019). ↩

77. https://www.ibm.com/blogs/policy/ibm-public-private-partnership-cybersecurity/ (Accessed July 29, 2019). ↩

78. https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/events/events-regarding-defence-and-security/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal (Accessed July 29, 2019). ↩

79. TRACFIN states that only 60 ICOs occurred in 2016, as compared to more than 2,000 ICOs in 2017 globally. ICOs, analogous to initial public offering, are instances where an entrepreneur(s) creates a blockchain for a new project (e.g., domain name, cloud services, auction website) through which they may issue tokens. These tokens are sold to potential investors, who can pay through virtual, and sometimes fiat, currencies, with most transactions occurring over the Ethereum blockchain. Tokens provide investors with rights, regarding the project, including dividends on income from the project and voting rights. The entrepreneur can then convert the virtual currencies obtained from investors into fiat-currencies in order to finance their operations, including hiring employees and obtaining equipment, among other activities. ↩

80. http://francopol.org/nc/ (Accessed July 20, 2019). ↩

81. Dupont, *La Régulation.* ↩