Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context: Executive Summary

R.V. Gundur¹, Michael Levi², Volkan Topalli³

¹Flinders University, ²Cardiff University, ³Georgia State University

Published on: Apr 16, 2021

DOI: 10.21428/cb6ab371.dd7a1c57

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

View the [Full Report](#)

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.

General Overview

This report surveys what is currently known about the financial transactions that cybercriminals conduct among themselves or demand/receive from their victims. Using multiple languages in addition to English, the project set out to examine what is known regarding the financial aspects of cyber-enabled and cyber-dependent crime, including fraud; theft; money laundering; extortion; selling/buying illicit drugs; selling/buying contraband and counterfeit goods. We sought to review the literature on cybercriminal business models, the role of virtual currencies and other technologies in these models, and how these crimes both interact and enable other economic crimes. We also reviewed the responses of law enforcement, private sector partners including cybersecurity firms, and others, nationally and internationally, to tackle the financial aspects of cybercrime, and what can be learned from these responses.

The report is divided into five sections and identifies the lessons learned across five linguistic searches: English, Russian, Chinese, Spanish, and French. Each section provides an overview of the state of play in the countries of interest. In addition, each section surveys the bodies and policies that are relevant to financial aspects of cybercrime and provides a critical review of the relevant literature.

In reviewing this literature, two analytical themes emerged. The first examined the processes and attributes of cybercriminal acts and what is known about the actors behind them, while the other examined the specific financial strategies employed to facilitate and benefit from profit-generating crimes. In both themes, authors prioritised examinations of the victim-facing parts of crimes (as opposed to what happens after a victim is victimised). They described how attacks happen: the vulnerabilities attackers exploit and processes of how crimes unfold, in broad terms. We identified little research where the data collected would facilitate the description and assessment of the enactment phase of cybercrimes (e.g. cybercrime scripts). Many claims within the grey literature – publications produced by corporate enterprises – lack methodological

rigour and both the facts and key messages asserted are difficult to verify. Moreover, most of the extant research ignores how cybercrime affects rapidly expanding internet markets in developing economies and their users. Taking these endemic limitations into account, this report provides the following.

First, it identifies and surveys the various financial ecosystems that exist in, or can be accessed by, cyberspace. It identifies six financial ecosystems: fiat currency; assets; digital currency; sanctioned alternative payments, such as mobile money, which operate under the approval and oversight of government regulators; unsanctioned alternative payments, which operate outside of government regulation; and bartering. Accordingly, this report considers how current regulation either covers or fails to cover non-cash transactions that may be used by criminal entrepreneurs to transact value electronically across these financial ecosystems.

Second, this review demonstrates that financial transactions in cybercriminal contexts are closely related to the crimes committed. To that end, we provide a typology of transactions that identifies who participates in a transaction, why transactions occur, how the transactions unfold, and what limitations transactions have from the viewpoint of the senders and recipients, who, depending on the transaction, will have differing needs based on whether they are offenders or victims. We show there are five principal transaction types related to criminal activities:

1. *willing transactions*, where both the payer and the payee are willing, knowledgeable participants getting, generally, what they expect;
2. *coerced transactions*, where payees/offenders compel or pressurise to varying degrees (e.g. through extortion or ransom) payers/victims to pay;
3. *filched transactions*, where offenders steal money or digital assets from their victims, some of whom may themselves be criminals (including tax evaders);
4. *laundering transactions*, where criminal actors obfuscate the origin of the proceeds of a crime and/or successfully cash out those proceeds into apparently legitimate, spendable currency; and
5. *bartered transactions*, where two parties exchange goods and/or services.

Importantly, this report concurs with Europol's assertion that fiat currency is still king: most identified transactions conducted or coerced by cybercriminal actors involve digital fiat currencies rather than digital non-fiat currencies, despite the disproportionate popular attention the latter receive. Usability in terms of (a) user (including victim) experience and (b) the capacity to spend are the key components determining the adoption of transactional methods.

Third, this report shows that the techniques employed by offenders are similar across the settings examined, with attackers leveraging the tools and technologies available to them. In short, offenders use the means available to offend; there is no indication that technical limitations or advantages are a driving force in whether or not an individual decides to engage in crime using ICT in some capacity. For example, if internet speeds are slow or access to technology and technological expertise is limited, then offenders use decidedly low-tech solutions, simply leveraging the ICT that is available. However, if internet speeds are fast and access to technology and technological experience are available, then offenders will develop skills and pursue behaviours that allow them to pursue larger paydays. Accordingly, it appears that offenders persist in using strategies that have proven successful. Given the low rates of detection, offenders do not innovate beyond what is necessary to stay in business and achieve their goals. The literature identifies offending patterns which seem to be consistent whatever language they use; chief differences which were identified existed in niche markets and value systems that were only locally or regionally available.

Fourth, this report indicates that in most cases cybercriminals specialise within particular processes along the chain of expertise required to enact a cyber offense (van Wegberg 2020). They are not responsible for developing and executing an entire attack or scam, particularly with larger, more involved, and more complex scams. Rather, offenders identify a niche area of expertise (e.g., social engineering, programming, transactional platform usage) and enact their expertise within that niche. They may act in concert with other offenders who specialise in other areas of the offending chain or leverage pre-existing technologies. There is an increasing growth in off-the-shelf solutions that allow cybercriminals to take existing structures and attack platforms and adapt them to their targets. Knowledge about how hard or easy it is to find co-offenders is modest outside of government-sponsored or high offender rate environments.

Finally, this report finds that, while there are several similarities across all linguistic regions studied, there are also important regional distinctions between cybercriminal markets in criminal behaviour, strategies, and objectives. Criminal behaviour is also strongly shaped by regulation, accessibility to payment platforms and technological resources, and domestic preference and accepted behaviour; consequently, there is a great deal of opportunity for formulating anticipatory cyber prevent policy to combat emerging trends in online financial cybercrime, such as a digital situational crime prevention approach that considers local technologies, such as the mobile money and commonly used operating systems; human vulnerabilities, which may vary depending

on socio-political circumstances; and, law enforcement capacities, which are variable in terms of capacity, communication, cooperation, and funding (Brewer et al. 2019).

Comparative Findings

Research: Availability, Quality, Capacity, and Limitations

Research on the transactional methods employed by cybercriminals and in cybercriminal contexts produced both by academics (the academic literature) and companies (the grey literature) is disproportionately in English, which may largely be a function of the stage of development of criminological, computer science, and cybersecurity research in the spaces reviewed. Nonetheless, the language of cyber is generally English, though there are significant non-English speaking user bases, who are unlikely to engage in English communications. Accordingly, this report sought to study all relevant outputs produced in English and four other major world languages: Russian, Chinese, Spanish, and French, to see if the focus, quality and volumes vary substantially from English language material.

Two questions informed this review. First, “How do cyber offender business models operate?” Second, “What are the current law enforcement and industry practices aimed at disrupting these business models?” In order to evaluate these questions, we catalogued 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 (both unidirectional and collaborative). To find relevant literature along these lines, we devised an array of search terms that 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 and included results published from 2014 through December of 2019.

We identified and retained 335 English-language articles; 111 Russian-language articles; 57 Chinese-language articles; 81 Spanish-language articles, and 37 French-language articles. Outside the Anglophone and Russophone literature, there was a lot of repetition of themes and conclusions first made in the English-language or, to a

lesser extent, Russian-language literature. Nonetheless, reviewing the non-English literature uncovers distinct concerns compared to those raised in the English literature regarding cybercrime vis-à-vis regulation, criminal ecosystems, and market concerns. In particular, these mention elements endogenous to local or regional markets that do not necessarily involve English-speakers, such as darknet markets, localised frauds, and regional behaviours and technologies such as payment habits and payment systems. Accordingly, this report shows that there are advantages beyond linguistic diversity to reviewing non-English literature if we wish to get a fuller grasp of international cybercrime.

Furthermore, this exercise showed that countries vary greatly in their willingness to document their cybersecurity strategies, concerns, insights, and capacities. Developed, wealthy countries tend to be more transparent, producing reports and studies by both government and private enterprise to generate insights into cybercrimes and their control. The literature reviewed suggests that developed countries are more likely to have educational facilities that can train personnel who, in turn, may become high-end cybercriminals or who could aid cybercrime investigation and prevention. In addition, developed countries are more likely to have public and private sector organizations that aid knowledge production and cybercrime defence. There can be consultancy and software sales, and bureaucratic growth as a by-product or even motive for taking cyberthreats seriously: indeed, this carries with it the risk of threat inflation for profit. By contrast, it appears from the literature and our efforts to examine educational resources in the countries surveyed in this report that emerging countries lack locally developed and supported educational facilities that can effectively train relevant professionals to combat cybercrime. As a result, they lack the local expertise to identify and respond to cybercriminal affairs, generally. Unlike some drugs or more ‘mainstream’ transnational crimes where there is active liaison and Global North interest in stimulating local anti-crime efforts, emerging countries are not frequent sites of international cybersecurity training, meaning that if locally-based professionals are to be trained, they must travel abroad to receive their training, which is frequently delivered in English or a language which is not their native one. Moreover, even when emerging countries have public-sector units that ostensibly address cybercrime, there is typically little information available publicly. It is likely that the lack of transparency in their reporting is an effort to avoid appearing incapable, or it may simply be a cultural tradition of closed enforcement culture. While international cooperation between countries is a common theme in government reports and policy documents,

accounts regarding how cooperation unfolds are limited to what is reported by developed countries.

The lack of information regarding what happens in emerging economies is a chief limitation of this report. While actors in emerging economies may be cast with suspicion for social engineering crimes, we see that the emerging technological uptake within emerging economies provides an immense opportunity for criminal entrepreneurs who have an increasing victim pool to target domestically as well as internationally. There is currently little research into the dimensions of known offending that targets victims in emerging economies, though it is likely to already be occurring, particularly as more countries increasingly adopt cashless payment solutions.

Financial Ecosystems in the Contexts Studied

This study identifies six financial ecosystems that are, or could be, of interest, to criminal entrepreneurs. These financial ecosystems overlap and can manifest in local, national, and international forms. The largest financial ecosystem is that of 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). We find that reported crimes that typically net the largest payoffs per crime target the taking or moving of fiat currency. Fiat currency is the target of most social engineering scams and frauds, regardless of where they occur, who the target is, or which language they use. Fiat currency is a good target given the number of existing systems that facilitate its transfer and payment; it is easily requested and transferred in its digital (non cryptocurrency) form, and arouses least suspicion among victims who do not realise they are being victimised: the essence of most scams, excluding extortion.

Digital fiat currency refers to digitally held and transacted fiat currencies, which represent the majority of fiat currency holdings in the world. Fiat digital currency is the most targeted by criminal actors, who have historically targeted domestic banking transaction systems and the SWIFT system. Both domestic banking systems and the SWIFT system have improved their capacity to identify theft and fraudulent transfers. That being said, relatively small-value transactions through money transfer services and prepaid debit cards are reported in each context reviewed within this report, as is

the use of money mules, who use their own accounts to store and transfer fiat currency at the command of a fraudster.

The **asset market** consists of possessable items that hold value, such as real estate and precious metals, and non-currency instruments, such as stocks, bonds, and debt. Most of the wealth in the world is held in offline assets. We did not find evidence that the asset market played any significant part in transacting value as a function of theft or scams in any country. It is possible that money is laundered through the asset market, e.g. through the disposal of the proceeds of crime; however, evidence as to how this occurs and estimates of scale was not presented in the literature reviewed for this report.

Virtual or cryptocurrencies are of considerable interest across the literature and are featured prominently in each language reviewed. They include digital currencies in videogaming ecosystems and virtual currencies, which are also commonly referred to as cryptocurrencies. Since the introduction of Bitcoin in 2009, hundreds of other cryptocurrencies have been introduced. Bitcoin still enjoys the largest market share. Bitcoin is pseudonymous, meaning that transactions can be ultimately traced, for example, if some information is revealed due to poor operational security. Nonetheless, it remains the most commonly requested cryptocurrency in illicit internet marketplaces and in ransomware demands. Other coins that are more privacy focused, such as Monero, Zcash, and Dash, have become more popular, though victims who are not technically aware may find them harder to negotiate, leading Bitcoin to be the default choice for inexperienced victims and collaborators, who appear to be the great majority.

Cryptocurrencies are most likely to be transacted for specific types of crime, such as cryptojacking, payment for illicit goods on cryptomarkets, and the ransoming of victims using ransomware. Importantly, ease of access to cryptocurrency also impacts whether a victim of ransomware or extortion can comply with an attacker's demands. There appears to be a decrease in extorting individuals, particularly in jurisdictions where acquiring cryptocurrency is difficult, such as China where cryptocurrency exchanges have been outlawed, making buying or selling cryptocurrency using local transactions almost impossible (Liu 2014; Guo 2015; Song 2013; Guo 2015; Yuan et al 2018). On the other hand, there appears to have been an increase in the cyber-extortion of cities and other public welfare venues such as hospitals, using their ill-matched integration of IT systems to find weaknesses. The value of most

cryptocurrencies is volatile, and crypto transactions of illicit value likely represent a small fraction of illicit money flows worldwide.

Criminal actors made comparatively small attempts in terms of value to transact or launder money using videogaming ecosystems, even though these transactions are generally not monitored by regulators.

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, which is increasing in popularity in places that have unbanked and underbanked populations. Popular systems include M-Pesa and Yandex.Money. Some of these payment systems are accepted in darknet and clearnet grey marketplaces that sell products that could be used to facilitate cybercrime.

Leveraging mobile money is where – particularly in emerging economies – we view the largest risk of attack over time – both in terms of probability and consequence. While transactions with mobile banking are small, when made at volume, perhaps in an automated way, as has been identified in Russia, these transactions can be used to launder money or to generate significant illicit revenue via theft, particularly given that many of these accounts are subject to weak know-your-customer (KYC) standards (Belousova and Chichkanov 2015, Vasyukov and Bulyzhkin 2017; Alexandrov 2018; Kumukov 2018).

Other notable alternative payment systems include voucher systems, such as paysafecard, MoneyPak, and Ukash, all of which have been cited in the literature as means to pay ransoms or to pay for products in illicit marketplaces.

Unsanctioned alternative payment systems are those payment systems that have endured outside any government regulation, such as hawala-type systems. Cryptocurrency, in its inception, was 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. Two notable payment systems that are now defunct, having either closed operations voluntarily or been shut down by law enforcement, are E-gold and Liberty Reserve. These systems provided unregulated transactional platforms that transfer value between actors, internationally, outside the banking system, without the need to provide verifiable information. At the time of

writing, WebMoney is the only system that appears to have persisted in this market space; however, it appears to comply with some KYC requirements, allowing it to continue to operate, which would also suggest that it is less-easily leveraged for illicit transactions compared to E-gold and Liberty Reserve.

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 possess. Bartering has also been observed, to a lesser extent, with prepaid debit cards or gift vouchers which are exchanged for products and services offered on the darkweb rather than for fiat or cryptocurrency.

The Operation of Cyber Offender Business Models

How do cyber offenders structure their financial operations?

Across the literature evaluated, we determined three key themes regarding offender business models. First, offenders leverage what is available to them. To that end, not all offenders have equal access to resources and technology or have equal skill levels. Some offenders may purchase tools and services to increase their capacity to attack. Moreover, there is a high degree of specialisation in cyberoffending; most offenders appear to focus on developing their skills to engage in one or two activities, and most offenders who target specific victims appear to have a type or class of victim – such as vulnerable people, like widows or the elderly, or high-value targets, such as high-level administrators in a business – they are most likely to target. Second, the crime committed determines how and whether money is obtained, transferred, converted, and cashed out. Third, if offenders require victims to act in order to gain income, the actions that offenders request victims to perform are typically within the realm of normalcy (e.g. everyday activities or known activities) for the victims. Across the literature, the crimes committed share many similarities; nonetheless, there are some regional nuances.

Players (Offenders/Attackers), Strategies, Products, and Services

There is no singular profile for a cyberoffender. When considering the financial aspects of cybercrime, three general classes may be usefully distinguished: vendors, consumers, and attackers. Vendors sell goods or services to consumers. Some consumers, such as those who purchase child exploitation materials or controlled substances, use products that are otherwise inaccessible legitimately. Others, such as

those who purchase exploit kits, services, or data, leverage those products for illicit purposes, sometimes as part of an attack.

There is a wide array of products (exploit kits, data, compromised VPNs) and services (hosting, DDoS attacks and other crimeware-as-a-service, money muling/ laundering) advertised to facilitate illicit purposes. Some are sold in grey marketplaces where the products are available for purchase using both standard payment services, such as credit cards, and non-standard payment services, such as cryptocurrency. Costs vary but do not appear to be high for basic technical products and services, such as SOCKS, compromised VPNs, bulletproof hosting, and remote desktop protocol (RDP). While we are unable to verify the veracity and validity of the products advertised in this review, our view is that at least some of the products advertised are legitimate. We were unable to establish costs and reliability of most laundering offers. We were also unable to trace the provenance of many of these offers, but it is our view that these services are likely to be hosted in places that have good ICT infrastructure and are targeted to actors who also have good ICT infrastructure.

Attackers are individuals who target victims to steal money, data, or other resources. Attackers' capacity to offend is limited by skill and access to resources, though it appears that attackers may have a preferred victim type that they are more likely to target coupled with an appropriate strategy. For example, there are low-scale fraudsters who may use largely unsuccessful, high-volume, low value attacks, such as using spam email to entice victims (e.g. the 419 scam). These attacks are unlikely to succeed for most users, but even extremely low conversion rates of low-value targets may be enough – given the volume of potential victims approached – to generate some income. (This income from crime has to be seen within the context of income available from legitimate work in the offender's jurisdiction.)

More sophisticated social engineers may attack specific high-value targets. For example, they may use more nuanced, complex techniques, tailored to the target, thereby increasing attack success rates and financial yield. The literature suggests that attackers who have skill, and perhaps additional access to victims' information, appear to eschew low-yield high-volume attacks with low payoffs for more targeted socially engineered-attacks. This report did not review pathways into offending specifically, but the Spanish and Russian reviews identified that youths are still recruited to engage in unsophisticated attacks or to be money mules; however, notable exceptions exist, such as the case of Marcus Hutchins who, as a teenager, developed the banking trojan Kronos.

Overall, in examining vendors, customers, and attackers, we see that criminal ecosystems are diverse in terms of the actors involved and the crimes that unfold. Actors include lone actors, coordinated criminal groups, and state-sponsored groups, all of whom may engage in scams and technical exploits. Across the literature, it is clear that offenders specialise based on their skill and access to technology, personalities, and entrepreneurial mindsets. The Anglophone literature focuses on a diverse array of offenders from low-tech social engineers, who use ICT simply to target potential victims *en masse* and to engineer a scam, to technically-involved thefts of money and data, and to disruptive or destructive actions that cause victims to suffer loss. Knowing this protect and prepare strategies should be prioritised furthering understandings of vulnerabilities and how to secure those vulnerabilities, particularly as new vulnerabilities emerge and begin to widen the scope for victimisation among distinct populations.

Similar patterns are evident throughout the literature. The Russophone literature identifies three clear offender business models. There are low-scale fraudsters, who may be independent operators, who target only Russians for modest sums, using social engineering methods; large-scale fraudsters, who may be composed of groups of attackers, who seek out larger-value targets both within Russian-speaking countries and non-Russian speaking countries, using both technical and social engineering methods; and state-backed hacker groups, who pursue political goals, such as disruption and data/intellectual property theft, using primarily technical methods. A similar division of offending was also observed in China. The Francophone literature identifies a distinction between (a) vendors who sold or rented botnets and malware and (b) monetisers who were able to convert stolen data into revenue or launder money. The Spanish literature discusses relatively low-tech scams that focus on defrauding victims or recruiting money mules. In sum, the pattern holds: opportunity shapes offender behaviour.

Financial Operations

The type of crime committed dictates what value instrument (e.g. fiat currency, cryptocurrency, vouchers, etc.) is transacted. Accordingly, in terms of obtaining money, fiat currencies are typically obtained from activities such as:

- Fraud, including leveraging financial data to make unauthorised purchases;
- Money muling;
- Phishing (though such attacks can seek to compromise any account that holds value, such as data, cryptocurrency, etc.);

- Social engineering scams; and
- Theft.

Cryptocurrencies are typically obtained via:

- Cryptojacking, the unauthorised use of computer resources to mine cryptocurrency;
- Ransomware;
- Extortion other than ransomware; and
- Sales of goods and services in illicit marketplaces.

Alternative payment systems, such as prepaid cards/codes and vouchers, have been requested by offenders to pay for:

- Extortion demands;
- Illicit purchases; and
- Ransom demands.

Alternative payment systems have also been used as a mechanism for shifting value internally or externally without the obvious signs of laundering.

Most of what we know centres on how money is acquired. The research in each language reported largely fails to address how money trails unfold after the initial crime takes place. This gap is, at least in part, due to the difficulty of doing offender-focused research; most of the literature uses open-source data and does not attempt to study the offenders themselves. This research is commonly underfunded by funding bodies. The literature consistently reports that – regarding the theft of fiat currencies – offenders usually execute multi-step transferring operations to engage in placement, layering, and integration processes. Common strategies use bank accounts both in local financial ecosystems and in various jurisdictions throughout the world, sometimes involving money mules. Some cashing out strategies leverage local policies and demands on officials. For instance, in China, it is reported that offenders take advantage of lax regulation and oversight to transfer and cash out money from new bank accounts, established using stolen or falsified credentials. Although the processes that form money laundering strategies of placement, layering, and integration are widely known, identifying their occurrence and the exact mechanisms that offenders use, particularly as they innovate to stay ahead of law enforcement, is difficult.

Similar transactional patterns have been observed to obfuscate the origins of cryptocurrencies that have been ransomed or stolen. Instead of mules, cryptocurrencies may be processed through tumbling services designed to obfuscate

the origins of the currency or through thousands of accounts; however, many of these services are scams and most do not truly launder the cryptocurrency without leaving forensic artifacts. Cryptocurrency is also more likely held by criminals, who may attempt to profit from the fluctuations of value or wait until there are more opportunities to purchase products that allow direct spending of the cryptocurrency, such as the purchasing of payment cards that can spend fiat currency. For example, in Russia it is estimated (with what degree of validity is impossible to verify) that only one third of stolen cryptocurrency is cashed out by criminal actors. It is unknown what impact Bitcoin and other cryptocurrency volatility has on the preferences of offenders – both those who do use crypto and those who do not.

In addition, several transactions of proceeds of crime make use of legitimate transaction platforms, such as traditional bank transfers, money transmission businesses, government-approved alternative payment systems, and e-payment systems. While regulation has sought to identify proceeds of crime as they enter the financial marketplace, clear and consistent mechanisms to investigate funds with questionable origins do not exist. However, an increase in KYC implementation appears to have limited the attractiveness of licit platforms to cash out in bulk. We view transaction mechanisms with low KYC protections (e.g. low-value accounts QIWI, Bitpesa, M-pesa, Yandex.Money, QQ coin) as a possible mechanism to launder and cash out money, if an actor can coordinate a large number of small transactions, as has been done in Russia via QIWI wallets. Moreover, the experience in China indicates that small-scale cybercriminals may demand and transact in readily disposable value instruments, such as online shopping vouchers and mobile phone credit. This underpins the reality that even with regulation, enforcement for small sums, unless a pattern of aggregation can be determined, may be more expensive than the loss itself. Accordingly, regulation may be a compliance-based exercise to ensure companies follow best-practice procedures. Moreover, if the size of these markets increase significantly, and is not explicable in terms of legitimate factors, then more serious disruption and closure techniques may have to be developed, including infiltration and social network analysis of background data.

What do we know about the extent of income or profits that offenders can make from cybercrime?

Estimates regarding the proceeds generated from cybercrime vary greatly, in the rare instances when they are offered. Russian industry experts estimate that Russian attackers generate between 50 to 100 million USD on the Russian market alone; however, Russia-based hackers earn the majority of their profits outside Russia and

there are no estimates of this value. One French study on offenders identified an actor earning approximately 10,000 USD per day over a 58-day period. There is a chronic lack of reporting of cybercrime; consequently, even when data regarding costs and losses exist, the inability to assess the number of actors involved in cybercrime, volume of attacks, and offender and activity success rates results means that there are no good estimates that would indicate an average or likely earnings value. Detection rates for, and action taken in response to, cyber-dependant and cyber-enabled crimes, particularly those that result in relatively modest losses, are low, meaning that criminal entrepreneurs who trade in these spaces likely do so with a high degree of impunity.

What is the role of virtual currencies in cyberoffender models?

Virtual currencies and alternative payment systems factor into crimes that demand a degree of anonymity for the sender or the recipient of the funds, such as purchases of illicit goods or services on an illicit marketplace or to pay a ransom request. In Russia, some offline services – such as couriering drugs – have been reportedly paid using cryptocurrency. However, the use of cryptocurrencies, and the prioritization of truly anonymous cryptocurrencies, is not sacrosanct.

Offenders will opt for less secure but more efficient financial transaction systems when doing so appears necessary or substantially easier to carry out the target crimes. Accordingly, while it is important to understand new developments, law enforcement must recognise that they new developments are likely minority activities, so unless they can be warned off at birth, law enforcement actors – especially given their own scarce resources – are best served focusing on interrupting established, more widely used technologies; unless such technologies are no longer acceptably efficient, offenders will continue to use them. In the Francophone literature, offenders reported selling stolen data and malware using widely used public payment systems, including credit cards, and pre-paid card services. A review of ransom requests of extant ransomware shows that Bitcoin, which is pseudonymous, is the overwhelming preference, with some ransomers abandoning more secure payment options in order to generate a larger number of payments. The preference for Bitcoin is an indication of its availability, spendability, and overall market share within cryptocurrency marketplace. In short, it is a comparatively stable asset compared to any other cryptocurrency available, especially when its value is rising.

Moreover, within some jurisdictions, where cryptocurrencies have been banned, such as China, trading in cryptocurrency is difficult, given the inability to cashout into fiat currency locally. Exchanges in the developing world exist, but given the preference for

fiat currency for most transactions that offenders will likely engage in during their day-to-day lives, it seems that most scammers based in the developing world focus on frauds that net fiat currency which can be more easily spent.

Though some cases have been identified, it is unlikely that many offenders convert fiat currencies into virtual assets to launder them, for a number of reasons. A record is produced by most exchanges which require KYC; the value of cryptocurrencies is volatile (though criminals may be as vulnerable as the public to beliefs in its rising trends in value), and the offline laundering processes of fiat currency continue to be effective. Whether virtual currencies are used in criminal transactions is contingent to the currencies' usability in licit settings; common, easily obtained and disposed of value instruments will be more commonplace than obscure ones. Accordingly, offenders' operational security through use of obscure cryptocurrencies is unlikely to be a significant driver. Moreover, even if cryptocurrencies are easier to transfer internationally, traditional money-laundering methods focusing on digital fiat currencies continue to be easier for most criminal actors by volume and value, and despite continuing efforts at suppressing money laundering, there is little evidence of serious impact of the controls.

How does cybercrime enable or interact with offline or apparently largely offline economic crimes, such as money laundering, fraud, and corruption?

Money laundering is a fairly automatic consequence of having generated any crime proceeds and not spending them on consumption in the short term. However, there does not appear to be much evidence suggesting that cybercriminal activity is being leveraged to facilitate offline manifestations of economic crimes, such as money laundering, fraud, and corruption. This is likely given the difficulty in converting cryptocurrency to fiat currency at volume without oversight, and also the because of the trouble to convert fiat crime proceeds into cryptocurrencies, whether those by cash or electronic funds. Offline economic crimes will likely persist in their current offline form so long as offenders are able to continue to be viable.

While the literature indicates that there may be capacity for the volume of money that is often in play with large-scale, offline economic crimes to be facilitated by digital technologies, there haven't been any cases that suggest this is currently happening at scale. What is more likely is that, as more financial transactions increasingly happen via cyber means, non-fiat systems will become more accepted as payment portals. In turn, as fiat currency transactions become less common, offline economic crimes will start to use digital technologies to transact. We have no indication as to how those

involved will develop strategies to obfuscate the nature of these transactions to auditors, to the extent that auditors are involved in their businesses. Nonetheless, the digitization of transactions may provide opportunities for different kinds of algorithmic-based oversight that allows for anomalies and patterns to be more quickly flagged for investigation. Such strategies are already being employed by banking systems to detect unauthorised transfers and other types of banking frauds. They are unlikely to identify all crime proceeds, but they may enable the accumulation of large proceeds if acted against rapidly and therefore reduce the volume of predicate crimes transacted in that medium.

Responses used by Governments, Law Enforcement, Private Sector Partners, and Other Interested Parties to Tackle the Financial Aspects of Cybercrime

How do political considerations, including political will and legislation, affect enforcement responses, including strategies employed, funding, and international cooperation?

Political interests, economic capacity, and domestic ICT development and infrastructure all play significant roles in any given country's enforcement responses. All of the countries surveyed in this project have a clear, stated interest in cybercrime and have named departments – notably Computer Emergency Response Teams (CERTs) – to respond to at least some forms of cybercrime, especially cyber-dependent crime. However, the capacity that these departments have to develop effective strategies to identify and respond to cybercrime domestically and transnationally varies greatly; some departments exist without any public facing information, regarding who they are or what they attempt to do.

Many developing countries are not transparent regarding their ICT limitations and capacities to respond to cyber-enabled or cyber-dependent cybercrime; we hypothesise that the lack of domestic training or international support will have a lasting effect in these jurisdictions in terms of how cybercriminal activity develops and how the public may be vulnerable to victimisation. While there may be international cooperation (and pressure to cooperate) buoyed by countries with developed ICT systems, and cybercrime and financial crime investigation capacity, these relationships are usually reported with little detail as to the extent of the cooperation or overarching capacity-building objectives of the partnerships. Cooperation varies greatly among countries, in part due to political interests. For instance, the Russian government is very concerned about cybercrime and information security treaties undermining or threatening the

sovereignty of the state. However, Russia appears to offer consistent cooperation vis-à-vis crimes associated with child exploitation.

Stimulated by inter-governmental organisations – notably the Council of Europe and the UN – and the CoE’s Budapest Convention, domestic legislation regarding *all* forms of cybercrime has increased but still varies greatly from country to country. Several countries have developed domestic legislation on cyberviolence, including bullying and harassment and online child sexual exploitation (See: <https://www.coe.int/en/web/cybercrime/domestic-legislation>). More generally, China and Taiwan both have extensive laws regulating cybercrime and money laundering, though China also defines cybercriminal behaviour more broadly than western countries, including activities such as distributing pornography and spreading rumours as crimes under its cybersecurity law. Latin American countries have developed legal frameworks designed to police specific cyberactions deemed to be criminal. Russia has done the same; however, some crimes that are notable in the literature, such as phishing, are not defined in Russia’s criminal code and therefore difficult to prosecute. There is little discussion in the publicly available literature regarding how states investigate or prosecute criminal actors engaging in transnational cybercrime within their jurisdictions, particularly as crimes may occur in several jurisdictions (and offenders in the same network may also be multi-jurisdictional). In addition, there is no indication of whether such investigations and prosecutions occur in jurisdictions like Russia and some western countries that do not extradite their own citizens or in developing economies that may not have robust legislation and investigative tools equipped to respond to cybercrime domestically or abroad.

Given the immense investment in preventing cybercrime – largely in part due to the difficulties in attributing malicious acts – a lot of monitoring and interdiction activities, such as examining network traffic and testing system vulnerabilities, are undertaken by private enterprise, given its vested interest in monitoring and protecting itself, rather than public law enforcement. There are still significant deficits in reporting mechanisms, particularly when the values lost are modest or involve individuals rather than companies. Priority has a large role in these deficits; reporting mechanisms vary greatly across jurisdictions with individuals and businesses often left with unclear avenues to report crimes. Plus, even when crimes are reported, individual losses subsumed by financial bodies are often dropped from police attention once the victim is compensated by those financial bodies. Moreover, the difference in priority is exemplified, for instance, in Russia where the state often views cybercrime as an external threat to the state’s stability rather than a threat to its ordinary citizens as

well. In short, there has always been a greater focus on national security risks from cybercrime – however variably defined – than on domestic crime risks, though the IoT may be shifting this risk perception. But cybercrime pursuit is expensive of resources and as Levi et al. demonstrated, is irrational unless mutual legal assistance and sometimes extradition and overseas asset recovery is plausible.

How do we increase costs to offenders and reduce the rewards of crime to offenders?

It is not feasible to increase the financial costs to offenders efficiently, though good security implementation, such as implementing best practice in regards to password usage and information backups, may increase the effort/temporal costs to offenders seeking to engage in certain activities and worsen the daily payoff. Nonetheless, the resources that can be leveraged for criminal activity are abundant and increasingly inexpensive. Moreover, there are large unknowns regarding activity, volume, and the people involved in various aspects of cybercrime, meaning that law enforcement efforts will continue to target high-value targets rather than creating general deterrence. Offender-focused research, such as ethnographic studies and interviews with caught offenders, could help shrink the knowledge gap along these processes and the people involved. Further information could help to improve situational prevention techniques that seek to understand the scripts of how crimes unfold and which respond to those stages, along with improved regulatory measures regarding transactions, including the regulations and the funding of oversight bodies to investigate potential regulations, are paramount to any effort to increase the viability of using digital means to engage in cycles of criminality.

The use of digital situational crime prevention measures has proven successful in reducing rewards to offenders vis-à-vis ransomware (Brewer et al. 2019). Better response mechanisms, including capacity to back up and restore and proactively seeking ransomware encryption keys, allow victims to refuse payment without suffering large-scale losses. Analyses of cryptocurrency wallets associated with ransoms have shown that many recent ransomware campaigns have not resulted in payments to ransomware operators. Improvements in terms of regulations that verify the use and employment of KYC standards and the enforcement of those regulations may also make some transactional methods unfeasible. This has been demonstrated with takedowns of alternative payment systems that, in the past, have been used for transferring the proceeds of crime and to make payments for illicit purposes, such as E-gold and Liberty Reserve. Accordingly, more rapid action responses may be needed to identify the threats posed by such mechanisms and – unless infiltration is selected as

the best course of action – close them down. As with fraud, the earlier the close down, the less the harm that is caused.

In addition, there is a need to diversify the array of actors equipped to respond to cybercrime, thus decreasing success rates and increasing the rates of detection. Private-public partnerships are commonly used to increase capacity in this regard. An example where this partnership has been successful is in combatting botnets. In one study, the number of detected malware cases in a country dropped after governments developed partnerships with private companies to counter cybercrime. Whereas law enforcement was ill equipped to handle the investigation and response of botnets, partnering with internet service providers provided a means to survey the online landscape and identify suspicious activity and victims of botnets. This top-down approach reduced the impact of botnets by identifying those affected and providing them with the tools needed to reduce their victimization.

What evidence is there to determine how effective disruption approaches are to preventing offenders obtaining, transferring, and cashing-out ill-gotten funds?

Estimating disruption of illicit transfers associated with cybercrime is not possible given the inability to estimate with any plausible range of accuracy the volume of such transfers at any specific time. What is clear is that increased regulation and enforcement have reduced some options previously available to cybercriminals which allowed them to transact the proceeds of their crimes easily. To that end, it is likely that increased KYC enforcement has forced at least some cybercriminals to engage in more sophisticated laundering strategies; we do not have a clear picture in terms of what these strategies are at present.

Nonetheless, this report indicates most jurisdictions – even those in developed countries but particularly in developing countries – still have comparatively limited investigative capacity to pursue cybercrime. Many, if not most, law enforcement bodies lack capacity and training necessary to prevent, discover, and investigate a broad array of cybercrime, meaning that the majority of cybercrimes is likely neither detected nor investigated. Estimates regarding investigated cases are as little as 1% of the likely total of cybercriminal activity.

The literature, however, clearly demonstrates that there is the forensic capability to investigate digital transfers, particularly of bitcoin, though those who have developed these techniques do not appear to engage with them frequently. Instead, authors writing on these techniques assert that regulatory frameworks are better responses

than tracing the cryptocurrency histories to limiting the ability to transact proceeds of crime at volume (van Wegberg 2020). Whatever approaches have potential at present, careful cost-benefit analysis at different levels of actually obtainable resource/skill levels is necessary to work out optimal practical strategies within constrained resources. ‘What works’ needs to be put in concrete settings.

What has come out of this that we didn’t really know already (foreign language) compared to the English lit?

In examining the foreign language literature on cybercrime, we acquired an understanding of the regional nuances regarding cybercrime and how governments and other interested actors prioritise their activities vis-à-vis cybercrime in terms of creating policy regarding and responding to cybercrime. The English literature focuses overwhelmingly on systems that are connected to the developed, English-speaking world without much regard to regional issues and how those issues may be representative of cybercriminal activity throughout the world, particularly when considering understudied emerging marketplaces.

Understanding regional issues is important for three reasons. First, disruptions in regional markets may have consequences further afield not only in terms of the countries but the markets affected. This is important in terms of global cooperation and law enforcement cyberstructures that may require international support for training and investigative capacity. Second, as business continues to be increasingly transnational, regional problems are unlikely to remain constrained or unique over time. Accordingly, regional problems may provide lessons that will be important as certain technologies, such as alternative payment systems, spread globally, including the diasporas in both developed and emerging economies. Third, understanding regional nuance may help international actors develop better prevent measures, by identifying and helping to interrupt “training grounds” where attackers hone their skills.

Whereas the English literature focuses on Russian actors who operate darkweb marketplaces, engage in largescale attacks, and attack non-Russian targets, the Russian literature highlights the role of low-scale fraudsters who attack domestic Russian targets. As a result, the Russian literature shows that there is a largescale manipulation of everyday users using social engineering techniques. Notably, 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, illustrating how the

asymmetric attention paid to large-scale attacks allows cybercriminals who target individuals to operate with a high degree of impunity. Everywhere, there is a problem in responding to domestic fraud and cybercrime complaints at scale, but some polities are less responsive than others to such crime and social problems.

The Chinese literature echoes the themes covered in the English language literature, namely that cybercrimes are specialised and that there are cybercriminal teams that coordinate in order to engage in large-scale attacks. Unlike the English literature, and whether due to self-censorship or for some other reason, there is no Chinese literature that implicates Chinese actors. However, the Chinese literature does elucidate trends that impact the domestic Chinese market. When considering domestic cybercrime, the Chinese literature shows that a substantial proportion of cybercriminals were young and lacked formal educational qualifications. Moreover, it showed that cybercriminals take advantage of inconsistent oversight and leverage the ease of opening bank accounts to cash out the proceeds of their crime. In addition, cybercriminals in China use existing communication platforms, such as WeChat or QQ, despite their privacy concerns. (There may be no communications media in China that do not present them with privacy concerns.) One important facet of cybercriminal transactions in China is the use of mobile payment systems and third-party payment systems, such as WeChat pay and Alipay, as well as the use of online shopping vouchers and mobile credit to transact value.

The English literature all but ignores the Hispanophone and the Francophone worlds. The Hispanophone literature indicates that the trends observed in the English literature, regarding much of the developing world, hold largely true for Latin American countries. Latin America generally lacks government capacity to respond effectively to cybercrime; legislation that identifies and facilitates the prosecution of cybercrime is slow to be promulgated. Nonetheless, several Spanish-speaking countries, including Argentina, Colombia, Mexico, Spain, Panama, Paraguay, Chile, and Costa Rica, have adopted national cybersecurity strategies. Defining cybercrime and regulating tools and financial instruments that attackers leverage to complete attacks is slow and uneven throughout Latin America; at the time of writing, there have not been any notable prosecutions.

The Hispanophone literature indicates that low-cost cyber-enabled crimes, such as social engineering, are relatively common. Accordingly, transactions associated with social engineering in Latin America are, like elsewhere in the world, often initiated by the victim and paid in fiat currency. Cryptocurrency is involved in transactions that

may be Ponzi schemes (against crypto-holders) or are spurred by ransoms. Ransoms have been also demanded via prepaid debit cards. Since technical crimes must target Spanish speakers, comparatively fewer ransomware strains appear to have impacted Hispanophone countries. Notable ransomware and malware executed in Spanish include Gataka, Zeus, Gameover, and SpyEyes.

The French review suggested that online offenders tend to have little experience, particularly in terms of the monetization of cybercrimes. The review also showed that criminal collaborations that form online tend to be highly volatile. Offenders who meet online encounter issues of trust, which make them susceptible to conflict and potential demise even before any external intervention. Finally, the French review, when speaking on Francophone cybercrime contexts, highlighted the importance of virtual currencies (e.g., online pre-paid cards) for illicit transactions, as opposed to virtual cryptocurrencies.

What are the implications for the Four Ps?

The Four Ps framework offers a helpful mechanism for sorting the contributions of control to different targets.

Prevent: The UK National Crime Agency has long expressed concern about young people being pressurised into a life of cybercrime and the importance of not giving redeemable young people the economic and social stigma of a criminal record that would prevent them from re-integrating into economy and society later. Hence the warning visits and letters to young people to inform them that what they had done was breaking the law, etc. The literature says relatively little about prevent experiments and efforts elsewhere.

However, there is a problem not just for the UK but for other countries, in that many cyber-offenders are based in different jurisdictions than their victims and targets, and such counter-criminal careers strategies would be extremely difficult to operate cross-border unless their 'home countries' were willing to see it. Understanding what is happening in other countries is quite key to understanding the cybercrime problem in its totality. No Global North country can reduce its cybercrime problem unless there is an effective effort to prevent people getting involved in cybercrime overseas. Whether 'walk softly but carry a big stick' approaches would work in corrupt and impoverished environments remains open to question. Not much evidence exists of such mechanisms being tried or of their effects, though just because they may not be practicable overseas does not mean that they should not be tried domestically. Nonetheless, it

appears that policies that increase accountability for reporting on the earnings of cryptocurrency funds that an individual holds have increased the difficulty of cashing out cryptocurrencies into fiat currencies. This is true in an increasing number of jurisdictions around the world, reducing the viability of being able to use those earnings for payments outside of the cryptocurrency financial ecosystem (van Wegberg 2020).

Pursue: It is a common understanding (or perhaps, belief), expressed most often in the UK, that the pursue function has limited mileage in dealing with cybercrimes. Attributing cybercrime to the actors responsible is an ongoing difficulty that law enforcement around the world faces in relation to the successful pursuit of allegations that can be tried fairly in criminal courts. The cost of pursuing cybercriminals means that except where convictions appear easy, available resources generally go to pursuing actors who pose the largest threats or cause the largest harms, and also pursuing threats that are capable of being dealt with through international action, including infiltration. The UK police and government are willing to express the notion that we cannot prosecute our way out of cybercrime (or indeed many economic crimes).

Legality principle countries such as Germany and Italy do not have this luxury, being legally bound to prosecute cases when there is sufficient evidence to do so. But again, we have the dilemma that setting aside resource issues, what can practically be done about offenders outside the jurisdiction, especially when the UK will no longer have the EU evidence or arrest warrant system to rely on. Council of Europe mutual legal assistance (MLA) mechanisms are not self-executing and there is reason to believe that other countries (possibly including the UK itself) may be reluctant to devote scarce resources to low value routine cases. Nevertheless, there are public reassurance rationales for public police interventions against cybercriminals, and more attention might be given to evaluating messaging and their effects on offenders, victims, and the general public. If the aim is modelled on HMRC approaches to fraud types, targeted interventions against different types of offenders might be considered strategically rather than as a relatively unplanned outcome of dispersed policing practices. Some UK as well as international investigations have revealed cryptocurrency wallets and have seized and liquidated them; however, money laundering investigations involving crypto are comparatively rare.

Protect: Protect seeks to insulate individuals, businesses, and public institutions from criminality. There is nothing obvious from the research reviewed here to add to what the NCSC is already trying to achieve. Assessing the impact of protection measures on

victimisation of individuals, businesses of different sizes, government and third sector bodies has not been done in an experimental way, and the general focus has been on social engineering rather than simply technical measures. A notable exception are improvements instated by SWIFT and ACH to catch fraudulent transactions before the transactions finalise; these efforts have led to a clear reduction in fraudulent transactions.

There exist a range of established ‘good practices’ of both risk assessment and prevention measures, but ensuring adherence – particularly regarding small-value transactions – has been a weak point. The published evidence on the impact of publicity campaigns is weak, as have been the primary measures employed for judging effectiveness (e.g. visits or at best multiple visits to prevention websites). Confirmation of payee measures adopted may reduce some Authorised Push Payments and ordinary mandate frauds, reducing the potential for cyberspace transfers. However, like measures adopted by banks to generate greater support for persons classified as ‘vulnerable’, published evaluations that meet high standards are very rare and fall into the ‘what’s promising’ rather than ‘what works’ category. The sustainability and roll-out of such processes are also in question.

Prepare: The bodies above to reduce the impact of criminality. It seems generally accepted that spending large amounts on prevention in advance of cyber-victimisation is organisationally difficult, and that this becomes a ‘teachable moment’ for serious prevention efforts. What is less clear is whether the victimisation of other firms in – by analogy of what HMICFRS would term a ‘family of forces’ – comparable businesses, government departments, and third sector organisations leads to adoption and sustenance of mitigation measures. Promoting resilience rather than first strike prevention may be a central part of cybersecurity, but how this applies to financial transactions in cyberspace is less clear.

What ongoing research gaps are there?

After conducting this literature review, we identify three ongoing gaps that require research: criminal opportunity, regulatory responses, and law enforcement responses, in diverse financial ecosystems; the disposal of the proceeds of cybercrimes of different kinds; and, criminal opportunity and victimisation in regional settings, particularly in the developing world.

There is a need to support 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, but regulatory responses have had significant impacts. Further studying these processes, and how they may be deployed with future financial technologies is critical. Nonetheless, 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, as are the basic technologies which facilitate these transactions, such as 2010s-era smartphones. This space must be a priority for future research.

The review of the literature shows that there is a glaring knowledge gap regarding 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. It is often asserted that cryptocurrencies are escalating in importance, but there is no obvious way of testing this claim (or the counter-claim that cash is still king) outside of the connections with cybercrimes themselves. (It should be borne in mind that many scams may have a mixed online and offline quality, so binary assumptions should be made with care.)

Finally, the review of the literature shows that cybercrime in regional and developing countries merits study. Given we live in a globalised world in which regional technologies often spread to other places, understanding, for instance, the vulnerabilities to the public and leveraging opportunities for offenders that new payment technologies present 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, both for the protection of the UK and for the protection of the UK's international aid recipient countries. Some examples include: how new users understand risk and risky situations online; how using old, out-dated technologies and hardware 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.

Works Cited

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.

Belousova, V. and Chichkanov, N. 2015. "Mobile Banking Adoption in Russia: What Incentives Matter?" In *Science, Technology, Innovation Economy*: Higher School of Economics.

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.

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.

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.

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.

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.

Vasyukov V. F., A. V. Bulyzhkin. 2017. "Nekotoryye Osobennosti Rassledovaniya Prestupleniy, Sovershayemykh S Ispol'zovaniyem Elektronnykh Platezhnykh Yedinit." [Some Peculiarities of Investigation of Crimes Committed Using Electronic Payment Units]. *Rossiyskiy sledovatel'*, no. 23

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

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.