Royal United Services Institute
for Defence and Security Studies

Occasional Paper

From Money Mules to Chain-Hopping

Targeting the Finances of Cybercrime

Anton Moiseienko and Olivier Kraft

From Money Mules to Chain-Hopping

Targeting the Finances of Cybercrime

Anton Moiseienko and Olivier Kraft

RUSI Occasional Paper, November 2018

Royal United Services Institute
for Defence and Security Studies

187 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 187 years.

Published in 2018 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, November 2018. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Acknowledgements

The research for this paper forms part of the Financial Crime 2.0 programme, which is generously sponsored by EY, Lloyds Banking Group and Refinitiv. The authors would like to thank all individuals and organisations who have shared their insight and expertise on issues covered in this paper. In particular, the authors would like to thank Professor Malcolm Chalmers, Professor Thomas J Holt, Professor Michael Levi and Adam Munro for helpful feedback on an earlier draft. Special thanks are also due to the RUSI Publications Team for their support in the production of this paper.

Executive Summary

THIS PAPER EXAMINES money-laundering techniques used by cyber-criminals and proposes measures that should be taken by UK policymakers, law enforcement agencies and regulated businesses to make it more difficult for such activities to go undetected.

Cybercrime has become a major category of financially motivated crime. It generates proceeds that in some cases amount to hundreds of millions of pounds. Moreover, it engenders a bustling underground economy where stolen data and services that facilitate cybercrime are traded.

Money forms a key part of cyber-criminals' motivation to engage in criminality. It is also their vulnerability. Since financially motivated crime inevitably involves money laundering, which refers to any use of the proceeds of crime, anti-money laundering (AML) measures can be used to target cyber-criminals. Financial investigation can be used to trace transactions and identify their beneficiaries. Criminal prosecution can target money launderers who help cyber-criminals transfer and use the proceeds of crime. Based on a review of publicly available information and interviews with subject-matter experts, this paper proposes ways of further strengthening these financial efforts against cybercrime.

Scope of the Paper

Cybercrime is a broad concept. This paper focuses specifically on the proceeds from hacking, malware infections (including ransomware) and distributed denial of service (DDOS) attacks. These are enabled by the existence of an underground criminal economy of services that facilitate cybercrime. In view of this, the paper also covers the proceeds of ancillary services that range from the provision of hacking, malware or DDOS attacks 'as a service' to money-laundering services.

Generation of Cyber-Criminal Proceeds

Since the form and amount of the proceeds often determine how they will be laundered, it is necessary to consider how cyber-criminals generate proceeds. This happens in a variety of ways, including:

- Taking over a bank customer's account or interfering with inter-bank payments, typically via Society for Worldwide Interbank Financial Telecommunication (SWIFT) intrusions, which leads to unauthorised electronic transfers of fiat currency (government-issued money such as US dollars or British pounds).
- Hacking ATMs or attacking banks' card-processing systems, which generates proceeds in cash. Attacks on card processing involve the deactivation of withdrawal and overdraft limits on cards held by criminals.

- Ransomware extortion, 'cryptojacking'[1] or theft of cryptocurrency, which all depend on cryptocurrency, such as bitcoin. The market in ancillary services is also dominated by cryptocurrency due to the perceived anonymity of transactions.

Laundering the Proceeds

Proceeds in Fiat Currency

The proceeds generated in government-issued fiat currency can either be digitally represented – for instance, funds in a bank account – or exist in physical cash. Proceeds from low-value, high-volume attacks that generate digitally represented fiat currency, such as account takeovers, are typically moved through several consumer bank accounts, which either belong to witting or unwitting 'money mules',[2] or have been hacked. In contrast, transferring large amounts of funds, such as those that originate from intrusions in inter-bank payments systems, requires corporate bank accounts and therefore involves the establishment of companies. In turn, cash-generating ATM hacking and attacks on card processing rely on a particular type of money mule to launder funds, namely individuals who pick up and transfer the cash.

Depending on the money-laundering scheme used, regulated entities and law enforcement agencies face different detection and investigation challenges. In particular, the use of money-mule accounts and high-velocity transactions by criminals requires financial institutions to identify such accounts and freeze the proceeds before they are withdrawn in cash. As discussed below, this requires a continuous reappraisal of approaches to data analysis and information sharing in relation to cyber indicators.

Proceeds in Cryptocurrency

The criminal provenance of cryptocurrency transfers is obscured through the use of mixers;[3] online gambling outlets that accept cryptocurrency; and, occasionally, rogue virtual currency exchanges. Although businesses that exchange cryptocurrency into fiat currency or vice versa will become regulated across the EU once member states implement the 5th Anti-Money Laundering Directive (5AMLD), member states are not required to extend the same rules to crypto-to-crypto exchanges. Such exchanges are open to abuse because they can convert traceable cryptocurrency such as bitcoin into privacy coins that are at the moment exceedingly difficult to trace (a process known as 'chain-hopping'). Furthermore, as the use of peer-to-peer (decentralised) exchanges, where users transact directly with each other, increases, so may

1. Exploiting another individual's or company's computational power to generate (mine) cryptocurrency for the criminal's benefit.
2. Unlike 'money laundering', 'money mule' is not a legal term of art. As discussed in Chapter I, it normally refers to people who wittingly or unwittingly send money on behalf of criminals, or even people whose accounts have been taken over by criminals.
3. That is, web services that are designed to ensure the anonymity of cryptocurrency transactions in return for a fee.

opportunities for laundering funds through them. Whether such exchanges fall within the scope of 5AMLD is questionable given that they only operate as intermediaries that connect users. Similarly, the use of mixers so far is not addressed in either the EU or the UK.

Key Areas for Further Action

Building the Knowledge Base

Improved understanding of how cyber-criminals launder the proceeds of their crime can produce a clearer intelligence picture of how they operate and, in particular, help identify key nodes of the enabling financial infrastructure. This will assist in focusing law enforcement and regulatory efforts. Additional analysis is needed to better understand:

- The modus operandi, identity and location of money launderers who provide such services as company incorporation to cyber-criminals.
- The modus operandi, identity and location of individuals who specialise in facilitating anonymous cryptocurrency transactions (for example, via mixers) and thereby wittingly or unwittingly facilitate the laundering of cyber-criminal proceeds.
- The ultimate use of the proceeds of cybercrime and their contact with the regulated sector, which can constitute a focal point for law enforcement and regulatory intervention.

Detecting Money-Mule Accounts

The use of money-mule accounts is ubiquitous in cybercrime involving fiat currency. Their detection poses challenges, especially if those accounts are several steps removed from the predicate crime. It is particularly difficult for financial institutions to identify accounts that cyber-criminals purchase from initially legitimate users. In view of these challenges, some financial institutions are exploring innovative methods of detecting money-mule accounts, such as:

- Real-time information sharing to trace criminal proceeds, including the proceeds from using stolen card data, down the chain of money-mule accounts after a known fraudulent transfer has taken place.
- Analysing a wide range of data points, including cyber indicators such as IP addresses and device IDs, to link related accounts. For instance, establishing that several ostensibly unrelated accounts are accessed from the same device can indicate money muling. Various data points, including cyber indicators, have already been used for those purposes, although the details cannot be disclosed in a public document. In this context, the reliability and standardisation of data points are crucial.

Whenever possible, the results of these initiatives should be communicated throughout the industry to share best practice, subject to necessary limitations on the sharing of confidential information or the details of an institution's business processes. If a particular type of information proves useful for analysis (for instance, cyber indicators), UK government stakeholders (especially the Home Office and the National Crime Agency [NCA]) and regulated entities should

verify to what extent it can be effectively shared via existing information-sharing arrangements. In addition, the NCA should consider introducing a standardised format for the inclusion by regulated entities of cyber indicators (such as IP addresses) in suspicious activity reports where available. This will facilitate the analysis of such data by law enforcement agencies.

Addressing Cryptocurrency-Related Risks

In line with the EU's 5AMLD, the UK will extend its AML regime to virtual currency exchanges and custodian wallet providers. Moreover, in October 2018 the Financial Action Task Force (FATF) extended its recommendations to 'virtual asset service providers', which include a broad range of cryptocurrency businesses beyond those to be regulated under EU law. This represents an appropriate moment for considering how the UK regulatory framework should extend to other cryptocurrency-related business models posing money-laundering risks, such as crypto-to-crypto exchanges, peer-to-peer (decentralised) exchanges and, potentially, mixers. Potential responses include either expanding the list of businesses subject to AML obligations on a case-by-case basis, as and when new business models arise, or using a flexible definition – for instance, of a 'money-service business' – that is capable of covering novel cryptocurrency businesses.

In addition to these measures, the UK government should provide guidance to regulated virtual currency exchanges on dealing with higher-risk counterparties, such as mixers or unregulated exchanges, and transacting in higher-risk cryptocurrencies, such as privacy coins. Such guidance will help exchanges assess the risks they face and prioritise mitigation measures.

Introduction

CYBERCRIME IS VIEWED as a serious threat to the prosperity and security of developed states, prompting the adoption of cyber security strategies across a range of countries.[1] Although some malicious cyber activities are carried out in the pursuit of military or political objectives,[2] a high proportion of cybercrime is financially motivated. According to one report, this was the case for 76% of all data breaches in 2017.[3]

Cyber threats, including those that emanate from serious and organised crime, are deemed to pose a Tier 1 national security threat in the UK.[4] The UK government's multi-pronged response is based on the three principles of 'Defend', 'Deter' and 'Develop'. In line with this, measures to ensure the security of the country's networks and data ('Defend') are complemented by efforts to 'detect, understand, investigate and disrupt hostile action' ('Deter').[5]

Accordingly, the UK government has vowed to dismantle the financial infrastructure of cybercrime and thereby '[add] friction to the criminal business model'.[6] Doing so requires the development of an intelligence picture of cybercrime-related money laundering, drawing on the resources of law enforcement agencies (LEAs) and the information supplied by businesses that are subject to AML obligations (regulated entities).

This paper seeks to advance the conversation on how this can be achieved. Specifically, it examines how cyber-criminals launder the proceeds of their offences, and analyses how the public and private sectors can contribute to the detection – and, ultimately, reduction – of such activities.

---

1. NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Security Strategy Documents', 22 January 2018, updated 8 October 2018, <https://ccdcoe.org/cyber-security-strategy-documents.html>, accessed 16 October 2018.
2. For an example, see the US indictment of 12 Russian intelligence officers who allegedly hacked the Democratic Congressional Campaign Committee and Democratic National Committee in 2016: US vs. Viktor Borisovich Netyksho et al., 'Indictment', US District Court for the District of Columbia, 13 July 2018, <https://www.justice.gov/file/1080281/download>, accessed 8 November 2018.
3. Verizon, '2018 Data Breach Investigations Report', 11th edition, p. 5, <https://www.verizonenterprise.com/verizon-insights-lab/dbir/>, accessed 16 October 2018.
4. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm9161 (London: The Stationery Office, 2015), p. 85.
5. HM Government, 'National Cyber Security Strategy 2016-2021', p. 25.
6. *Ibid*, p. 48.

Scope

This paper focuses on the proceeds of three types of cybercrime: hacking; malware infection (including ransomware); and distributed denial of service (DDOS) attacks. Chapter I discusses in greater detail the reasons behind examining these types of cybercrime to the exclusion of, for example, online fraud.

These offences are closely connected to a cyber-criminal economy where criminals can buy or sell stolen data obtained through data breaches as a consequence of hacking or malware infections. The proceeds of that trade fall within the scope of this paper. The cyber-criminal economy also encompasses many service providers catering to the criminal demand. As a result, this paper also looks at the proceeds from selling ancillary services, such as: the provision of hacking, malware or DDOS attacks 'as a service';[7] the provision of botnets[8] for DDOS attacks or malware distribution; the supply of products that shield malware against detection; bulletproof hosting;[9] escrow services;[10] and money-laundering services.

Although the paper focuses on UK responses, the international nature of cybercrime means that many of the findings and some of the recommendations are likely to also apply in other countries facing a significant threat of profit-driven cybercrime.

Relevance

The necessity for criminals to move and invest the proceeds of crime is the main rationale for global efforts against money laundering, in other words against conduct that relates to disposing of criminal proceeds and that can be prosecuted independently of the underlying illicit activity (predicate crime).

Moreover, regardless of whether a suspect is charged with money laundering, financial investigation can be a helpful component of the overall investigatory strategy into most forms of profit-driven crime. The Financial Action Task Force (FATF) defines financial investigation as:

> an enquiry into the financial affairs related to a criminal activity, with a view to:
>
> - identifying the extent of criminal networks and/or the scale of criminality;
> - identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and

7. See 'Defining Cybercrime' in Chapter I for definitions.
8. Networks of compromised computers controlled by the criminal. See 'Box 2: Botnets' for more details.
9. The hosting of illicit content, such as cyber-criminal forums or command-and-control centres for botnets.
10. Acting as a trusted party for two transacting criminals.

- developing evidence which can be used in criminal proceedings.[11]

All these objectives can be relevant in the context of cybercrime. For instance, tracing the financial flows from several ransomware attacks to the same cryptocurrency wallet shows that they may have been committed by the same person or group.[12] This helps identify the genuine scale of criminality and allocate law enforcement resources to tackling the most prolific criminal actors.

Financial investigation can also contribute to establishing the identities of previously unknown cyber-criminals. In cases of bank account takeovers, tracing down money mules, who wittingly or unwittingly withdraw and send funds on behalf of a cyber-criminal, can lead LEAs to that criminal, for instance by intercepting communications between the criminal and the money mules.[13] For this reason, criminals' money trails can be their vulnerability, and some LEAs routinely use financial investigations to follow the money in cases of bank account takeovers via malware infections.[14]

11. Financial Action Task Force (FATF), 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', updated October 2018, Interpretive Note to Recommendation 30, p. 98. On the role of financial investigation in policing, see Helena Wood, 'Every Transaction Leaves a Trace: The Role of Financial Investigation in Serious and Organised Crime Policing', *RUSI Occasional Papers* (September 2017).
12. Author Skype interview with a cyber security academic, March 2018.
13. Author interview with a law enforcement officer, London, May 2018.
14. Author telephone interview with a law enforcement officer, July 2018.

Box 1: Virtual Currency, Cryptocurrency and Virtual Assets

The EU's 5AMLD defines virtual currency as:

> a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

Individual units of virtual currency are often referred to as 'tokens' or 'coins'.

The FATF initially distinguished between decentralised virtual currency, which operates on the basis of cryptography and is therefore known as cryptocurrency, and centralised virtual currency. Unlike centralised virtual currency, such as WebMoney or Perfect Money, cryptocurrency does not have a central issuer and therefore does not have a central chokepoint susceptible to regulation. The first and most widely adopted cryptocurrency is bitcoin, but there are now more than 1,500 other cryptocurrencies, known as 'alt-coins'. (This paper follows the common practice of capitalising Bitcoin when referring to its technical protocol or the payment infrastructure while using lowercase in relation to bitcoin as a currency.)

Each bitcoin transaction is entered on the blockchain, a publicly available distributed ledger than contains the record of all transactions. Users on the blockchain are only identified by their alphanumeric 'public' cryptography keys. This pseudonymous nature of Bitcoin poses its main financial-crime risk. On the other hand, Bitcoin's transparent blockchain enables tracing of all transactions, although often at considerable cost and expense. Privacy focused coins, such as Monero, Dash and Zcash, use various techniques to reduce the traceability of transactions.

In October 2018, the FATF amended its Recommendations to include a definition of 'virtual assets', referred to as 'a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'. Although the FATF does not explicitly address the use of the term 'asset' instead of 'currency', several jurisdictions prefer this wording due to cryptocurrencies' widespread use for speculation as opposed to payment medium.

Sources: Council of the European Union, 'Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU', Official Journal of the European Union *(L156/43, 19 June 2018); FATF, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', June 2014, p. 5; 'All Cryptocurrencies', <https://coinmarketcap.com/all/views/all/>, accessed 16 October 2018; David Carlisle, 'Virtual Currencies and Financial Crime: Challenges and Opportunities',* RUSI Occasional Papers *(March 2017), pp. 1–5, 16; Tom Keatinge, David Carlisle and Florence Keen, 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses', European Parliament, Study for the TERR Committee, May 2018, pp. 32–33; FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', Glossary, p. 124.*

In cases involving cryptocurrency, LEAs may be able to de-anonymise suspected criminals' wallet addresses by clustering related cryptocurrency addresses (for instance, based on them being used in the same ransom notice) and connecting them to an individual based on various attribution clues, such as those found on public internet forums or devices seized from other suspected criminals.[15]

Financial investigation is essential to locating, seizing and ultimately confiscating assets derived from cybercrime. Successful instances of confiscation of the proceeds of cybercrime in the UK include the civil recovery of property worth £1.6 million from the partner of an alleged party to the Dridex conspiracy,[16] as well as the confiscation of £500,000 of bitcoin from Grant West aka Courvoisier, an individual who had stolen and sold personal customer data from a range of UK-based companies.[17]

In addition to financial investigation, another component of financial efforts against cybercrime is identifying the key services or institutions that cyber-criminals rely on to launder the proceeds of their activities. Making those services or institutions more difficult to access can render cybercrime less lucrative and, ideally, reduce the incentive to engage in it.[18]

Audience

The intended audience of this paper includes policymakers in the areas of cyber security and financial crime, law enforcement agencies, and compliance staff in regulated entities, including financial institutions and virtual currency exchanges.[19]

Methodology

This paper is based on a review of the available literature, interviews and a workshop. The literature review covered materials of relevance to the financial dimension of cybercrime, including: governmental publications; reports by international bodies (such as the Council of Europe, Europol and the FATF); court materials such as judgments or indictments; reports by

15. Masarah Paquet-Clouston, Bernhard Haslhofer and Benoit Dupont, 'Ransomware Payments in the Bitcoin Ecosystem', paper presented to the 17th Annual Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, 18–19 June 2018, p. 3.
16. National Crime Agency, 'Criminal Assets Worth £1.6m Recovered in Civil Case', 21 April 2017.
17. *UK Breaking News,* 'Half a Million Pounds Worth of Bitcoin Seized from Prolific Hacker', 25 May 2018; Crown Prosecution Service, 'Prolific Computer Hacker Jailed for 10 Years', 25 May 2018.
18. One of the FATF's criteria for an effective AML system is that 'the prospect of detection, conviction, and punishment dissuades potential criminals from carrying out proceeds generating crimes and money laundering'. See FATF, 'Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems', updated February 2018, p. 111.
19. In line with the EU's 5AMLD, which speaks of 'providers engaged in exchange services between virtual currencies and fiat currencies' (Article 1), this paper uses the term 'virtual currency exchange' rather than 'cryptocurrency exchange'.

cyber security companies; publications by non-governmental bodies; and academic papers. These materials were identified based on an open-source search of relevant key terms; references in other publications; and recommendations by subject-matter experts with whom the research team interacted during interviews or at conferences.

This research also involved 44 non-attributable interviews, which are cited throughout the paper with reference to the interviewees' area of expertise but without disclosing their identity. RUSI researchers interviewed representatives of UK and overseas LEAs, financial institutions (including banks and money-service businesses), cyber security companies and independent experts. Two LEAs chose to provide written replies to RUSI's questions rather than take part in a research interview. Relevant individuals and organisations were identified on the basis of their area of work, publication output, existing contacts with RUSI or recommendations by other interlocutors.

The objectives of the interviews were twofold: to obtain up-to-date information or opinions on issues that were not sufficiently addressed in the existing literature; and, if applicable, to discuss potential improvements to ongoing efforts against cybercrime in the area of the interviewee's expertise. Due to their specialist nature, some of the issues that arose during the research for this paper were only addressed by one or two interviewees. When possible, these were verified against other publicly available information that either supported such statements or was broadly consistent with them. Although some caution is necessary when relying on these statements, they provide helpful insight into the issues discussed in the paper.

To ensure the accuracy and relevance of RUSI's findings and recommendations, provisional findings and recommendations were discussed at a workshop held in London on 30 May 2018 with the participation of representatives of UK LEAs, government agencies, financial institutions, cyber-security companies, and academia.

An inevitable methodological limitation is that analysis of cybercrime may be skewed by a focus on high-profile cases about which better data is available. To the best extent possible, this was mitigated by having a broad selection of interviewees from a cross-section of public agencies and private institutions, and by covering a wide range of relevant literature. Furthermore, as with any other research on crime, this paper can only draw on materials about cybercrime that has been reported.

Structure

Chapter I outlines the types of cybercrime covered in this paper, explains the reasons for focusing on them and discusses their principal characteristics that affect the financial response to cybercrime. Chapter II analyses how cyber-criminals generate, launder and use the proceeds of crime. Chapter III examines the current efforts to target the finances of cybercrime and identifies key areas for further action. The paper ends with conclusions and recommendations.

I. The Financial Dimension of Cybercrime

THIS CHAPTER PROCEEDS in two steps. First, it explains what types of cybercrime this paper examines. Second, it sets out why these crimes are increasingly being treated as predicate offences for money laundering and what value financial investigation adds in the context of those offences.

Defining Cybercrime

The origins of the term 'cybercrime' reach back to the neologism 'cyberspace' coined by William Gibson in his science-fiction story 'Burning Chrome' in 1982.[20] Under a wide definition, cybercrime includes various types of crime committed through the use of computers or telecommunication systems such as the internet.[21] Since there is no agreement on how central the 'cyber' element should be, research and policy documents on 'cybercrime' often look at different phenomena, depending on the exact definition used.[22]

This section describes the types of cybercrime and ancillary services that fall within the scope of this paper. It also explains where these types of cybercrime are situated within the taxonomy of cybercrime adopted by the UK government and the Budapest Convention (see below).

Hacking, Malware Infections and DDOS Attacks

Hacking

The Crown Prosecution Service (CPS) defines hacking as 'the unauthorised use of, or access into, computers or networks by exploiting identified security vulnerabilities'.[23] Although some definitions of vulnerabilities encompass non-technical vulnerabilities such as employees

20. Lennon Y C Chang and Peter Grabosky, 'Cybercrime and Establishing a Secure Cyberworld' in Martin Gill (ed.), *The Handbook of Security,* 2nd edition (London: Palgrave Macmillan, 2014), p. 322; William Gibson, *Burning Chrome and Other Stories* (London: Harper Collins Publishers, 1995).
21. Chang and Grabosky, 'Cybercrime', p. 323.
22. Home Office, 'Understanding the Costs of Cybercrime: A Report of Key Findings from the Costs of Cybercrime Working Group', Research Report 96, Home Office Science Advisory Council, 2018, p. 12.
23. Crown Prosecution Service (CPS), 'Cybercrime – Prosecution Guidance', <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>, accessed 16 October 2018.

forgetting to switch off their computers,[24] hacking in a narrow sense involves the exploitation of computer vulnerabilities,[25] or weaknesses in the computational logic.[26]

Malware

As defined by the OECD, '[m]alware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners'.[27]

Unless a user is tricked into voluntarily executing a malware file, the cyber-criminal needs to gain access to the target computer in the first place by using an exploit, which delivers and executes a malware programme, also called a 'payload'.[28] An increasingly widespread variety of malware, known as 'ransomware', encrypts the user's files until a payment is made to the cyber-criminal.[29] Also of particular relevance to this research are Trojans, which are disguised as legitimate files and execute their malicious payload once downloaded by the user.[30]

Since malware infections always entail unauthorised use of the targeted computer, they are a type of hacking. Conversely, hacking typically – albeit not universally[31] – requires malware infection. The use of both terms in this paper is intended to emphasise the focus on the proceeds of all types of hacking and malware infections, including ransomware.

DDOS Attacks

DDOS attacks constitute 'attempts to render a computer system unavailable to users through … saturating the target computers or networks with external communication requests' that

24. See Julie J C H Ryan, 'How Do Computer Hackers "Get Inside" a Computer?', *Scientific American*, undated.
25. Thomas J Holt, Adam M Bossler and Kathryn C Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction,* 2nd edition (Milton Park and New York, NY: Routledge, 2018), p. 71.
26. National Vulnerability Database, 'Vulnerabilities', <https://nvd.nist.gov/vuln>, accessed 16 October 2018.
27. OECD, 'Malicious Software (Malware): A Security Threat to the Internet Economy', Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, 2008, p. 10.
28. Wendy Zamora, 'What Are Exploits? (And Why You Should Care)', Malwarebytes Labs, 29 March 2017, <https://blog.malwarebytes.com/101/2017/03/what-are-exploits-and-why-you-should-care/>, accessed 16 October 2018.
29. EC3, 'Police Ransomware: Threat Assessment', February 2014.
30. Holt, Bossler and Seigfried-Spellar, *Cybercrime and Digital Forensics,* pp. 131–41.
31. For instance, structured query language (SQL) injections do not require malware; see Michael Buckbee, 'Understanding SQL Injection, Identification and Prevention', Varonis Inside Out Security, 12 June 2016, <https://blog.varonis.com/sql-injection-identification-and-prevention-part-1>, accessed 16 October 2018.

are carried out by many computers at the same time.[32] In contrast to 'simple' denial of service (DOS) attacks that come from one IP address, DDOS attacks involve communication requests from a large number of IP addresses.

To launch DDOS attacks, some perpetrators take over a multitude of computers (known as 'bots') by infecting them with malware and then using the resulting 'botnet' to overwhelm the targeted system. As a consequence, such DDOS attacks involve both malware infections, to create a botnet, and DOS attacks against the target. The Avalanche Network, dismantled by joint US-German efforts with the involvement of Europol, is an example of a group that provided both botnets and money-mule networks to other criminals.[33]

Another widespread method of executing a DDOS attack involves reflection and amplification: 'These attacks are based on the principle that an attacker sends a relatively small request to a server, crafted with the spoofed IP address of the intended target (reflection), and for which the response is much larger than the request (amplification)'.[34]

DDOS attacks can be purchased online from websites known as 'booters' or 'stressers', which occasionally maintain that they merely enable customers to stress-test the robustness of their own websites. Although booters/stressers were used in the past to carry out DDOS attacks by means of botnets and are occasionally still used for this purpose,[35] at the moment such websites typically rely on reflection and amplification attacks.[36] One example of such a website is Netspoof, which accepted payments via PayPal and in bitcoin before being taken down in December 2016.[37]

32. Cybercrime Convention Committee, 'T-CY Guidance Note #5: DDOS Attacks', T-CY (2013)10E Rev, 5 June 2013, p. 3.
33. FATF, 'Professional Money Laundering', July 2018, p. 24.
34. Jose Jair Santanna et al., 'Booters – An Analysis of DDoS-as-a-Service Attacks', paper presented to the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, Canada, 11–15 May 2015, p. 3.
35. Cloudflare, 'What is a DDoS Booter/IP Stresser? | DDoS Attack Tools', <https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/>, accessed 16 October 2018.
36. Santanna et al., 'Booters – An Analysis of DDoS-as-a-Service Attacks', p. 3.
37. National Cyber Security Centre (NCSC) and National Crime Agency (NCA), 'The Cyber Threat to UK Business: 2016/2017 Report', 2017, p. 6; see also Europol, 'Joint International Operation Targets Young Users of DDOS Cyber-Attack Tools', press release, 12 December 2016, <https://www.europol.europa.eu/newsroom/news/joint-international-operation-targets-young-users-of-ddos-cyber-attack-tools>, accessed 16 October 2018.

Box 2: Botnets

A crucial type of cyber-criminal services is the provision of botnets, networks of compromised computers controlled by the criminal. They can be used to either distribute phishing emails, which often contain malware, or launch DDOS attacks. For instance, in January 2017 a British citizen allegedly employed the Mirai malware to assemble a botnet that he used for DDOS extortion against two UK banks. In December 2017 the US Department of Justice prosecuted a Romanian couple for allegedly trying to take control of 123 computers of the Metropolitan Police Department in New York to distribute the Cerber ransomware. In these cases, the perpetrators sought to assemble their own botnets, although botnets can be rented from others.

Sources: Emma Dunkley, 'Briton Extradited from Germany to Face Bank Hacking Charges', Financial Times, *30 August 2017; US vs. Mihai Alexandru Isvanka and Eveline Cismaru, 'Affidavit in Support of a Criminal Complaint', United States District Court for the District of Columbia, 1:17-mj-0095RMM, 11 December 2017, para. 22; Lillian Ablon, Martin C Libicki and Andrea A Golay,* Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar *(Santa Monica, CA: RAND Corporation, April 2013), p. 21.*

Ancillary Services

Aspiring cyber-criminals need not write their own malware or assemble a botnet to carry out a cyber attack. These can be purchased from more experienced and sophisticated service providers. In 2017, the UK's National Cyber Security Centre (NCSC) and NCA explained the benefits to criminals of the 'cybercrime as a service' (CaaS) model:

> The developer is less exposed to the risk of deploying the malware itself but will still generate income, whilst the user gains access to tools and techniques that they would not normally be able to develop or use. As such the cyber-as-a-criminal-service [sic] model will continue to expand in terms of users and the range of services offered, especially with the source code of some malware variants freely available (for example, Mirai).[38]

The same report predicted that entry barriers to cybercrime will keep diminishing as less sophisticated criminals are able to purchase the services of tech-savvy collaborators.[39] The proliferation of malware for sale has prompted some states, including the UK and the US, to criminalise the supply of malware to others.[40] In addition to buying malware, available services that cyber-criminals tend to purchase include the following:

- **Counter-antivirus and cryptor services,** which hinder malware detection.[41]

38. NCSC and NCA, 'The Cyber Threat to UK Business: 2016/2017 Report', p. 7.
39. *Ibid*.
40. Holt, Bossler and Seigfried-Spellar, *Cybercrime and Digital Forensics,* pp. 158–61.
41. NCSC, 'Cyber Crime: Understanding the Online Business Model', April 2017, p. 8.

- **Bulletproof hosting services,** which refer to the hosting of illicit content on servers either intentionally or as a consequence of not verifying the customer's content.[42]
- **Escrow services,** which involve acting as a trusted party for two transacting criminals.[43]
- **Drop services,** which can either refer to money laundering broadly speaking,[44] or specifically to reshipment scams. The latter involve witting or unwitting money mules (also known as 'drops') who receive on behalf of the criminal the goods purchased online using stolen card details.[45]

Together with the provision of malware and botnets, all these services fall within the scope of ancillary services listed in the Introduction. Although they all facilitate cybercrime in one way or another, not all are cyber-criminal by nature. In particular, money-laundering services are in high demand among cyber-criminals. Recent research suggests that 'cash-out schemes' – that is, goods and services that can be used for money laundering – are the most widely offered category of non-drugs products on the Dark Web, the segment of the internet that cannot be indexed by search engines and requires software such as TOR to access.[46] Although these statistics cover dual-use items that can also be used to commit predicate crimes (such as credit card or bank account details), other sources also point to an increase in the number and variety of money-laundering services on offer online.[47]

Taxonomies of Cybercrime

UK Government Taxonomy

UK governmental publications distinguish between cyber-dependent crime, which can only be committed using computers or the internet, and cyber-enabled crime, which is facilitated by their use but does not require it.[48] The three principal types of cybercrime covered by this research

42. Max Goncharov, 'Criminal Hideouts for Lease: Bulletproof Hosting Services', Trend Micro, 2015, p. 15.
43. NCSC, 'Cyber Crime', p. 8.
44. *Ibid.*
45. Shuang Hao et al., 'Drops for Stuff: An Analysis of Reshipping Mule Scams', paper presented at CCS'15, 12–16 October 2015, Denver, Colorado, p. 6; 30–40% was mentioned as a mule herder's fee in an author interview with a cyber-security expert, London, April 2018.
46. Nicolas Christin, 'After the Breach: The Monetization and Illicit Use of Stolen Data', testimony before the Subcommittee on Terrorism & Illicit Finance, Committee on Financial Services, US House of Representatives, 15 May 2018, p. 7.
47. Max Goncharov and David Sancho, 'The Panamanian Shell Game: Cybercriminals with Offshore Bank Accounts?', *Trend Micro Security Intelligence Blog,* 9 May 2016.
48. Mike McGuire and Samantha Dowling, 'Cybercrime: A Review of the Evidence', Home Office Research Report 75, October 2013, Chapters 1–2. Other taxonomies of cybercrime are summarised in E-CRIME, 'The Economic Impacts of Cybercrime: D2.1 A Report on Taxonomy and Evaluation of Existing Inventories', November 2014, pp. 8–24.

(hacking, malware infections and DDOS attacks) fall within the notion of cyber-dependent crime as per the UK's Serious and Organised Crime Strategy 2013.[49]

The same is true of such ancillary services as the provision of malware, the provision of botnets, the supply of products that shield malware against detection, and bulletproof hosting. In contrast, escrow services and money-laundering services do not constitute cyber-dependent crime. However, they form part of the cyber-criminal economy and, in view of the focus of this paper on the financial dimension of cybercrime, are considered here.

The Budapest Convention

Internationally, the Council of Europe's Convention on Cybercrime, known also as the Budapest Convention, sets the benchmark for defining cyber-related offences. As of November 2018, 61 states were parties to the Convention, including non-Council of Europe states such as the US, Australia, Canada and Israel.[50] The Convention does not define 'cybercrime' per se but lists a number of offences that states parties must criminalise.

Table 1: Offences Under the Budapest Convention

Category	Offences
Offences against the confidentiality, integrity and availability of computer data and systems	Article 2 – Illegal access Article 3 – Illegal interception Article 4 – Data interference Article 5 – System interference Article 6 – Misuse of devices
Computer-related offences	Article 7 – Computer-related forgery Article 8 – Computer-related fraud
Content-related offences	Article 9 – Offences related to child pornography
Offences related to infringements of copyright and related rights	Article 10 – Offences related to infringements of copyright and related rights

Source: Council of Europe, 'Convention on Cybercrime', European Treaty Series No. 185, adopted on 23 November 2001, ratified by the UK on 25 May 2011.

The types of conduct examined in this paper are likely to fall within the category of offences against the confidentiality, integrity and availability of computer data and systems under the

49. HM Government, *Serious and Organised Crime Strategy*, Cm8715 (London: The Stationery Office, 2013), p. 22. The 2018 *Serious and Organised Crime Strategy* does not refer to cyber-dependent or cyber-enabled crime. However, it refers to the 'National Cyber Security Strategy 2016-2021', which uses both terms (see p. 17).
50. Council of Europe, 'Chart of Signatures and Ratifications of Treaty 185', <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=hwAUbbPv>, accessed 21 November 2018.

Budapest Convention. In the UK, they are likely to be punishable under the Computer Misuse Act 1990 and are typically prosecuted under that Act.[51]

However, depending on the applicable legal framework and prosecutorial strategy, cybercrimes may not always be prosecuted as such. For instance, hacking can be punishable as wire fraud in the US.[52] In the UK, Grant West, a hacker who had stolen 'financial data and passwords belonging to tens of thousands of people in order to sell the information on the dark web', was convicted not only of offences under the Computer Misuse Act 1990 and money laundering, but also of conspiracy to defraud.[53] Notwithstanding some variety in possible legal classifications of cybercrime, terms such as 'hacking' provide helpful '"act descriptions" that may be used as a starting point for analysis and discussion'.[54]

This section discusses the factors that highlight the need for a financial response to cybercrime: the scale of its revenues; the international nature of cybercrime; the demonstrable value of financial investigation in cybercrime cases; and the expanding institutional and legal capacity to apply financial investigation to cybercrime.

Scale of Cyber-Criminal Revenues

According to a 2018 report, hacking and malware infections accounted for the largest numbers of data breaches in 2017, while DDOS attacks resulted in the highest number of cyber incidents.[55] Most of these activities were financially motivated.[56] However, despite the centrality of money

51. CPS, 'Cybercrime - Prosecution Guidance', <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>, accessed 16 October 2018; see also Michael J L Turner, 'Computer Misuse Act 1990 Cases', 2018, <http://www.computerevidence.co.uk/Cases/CMA.htm>, accessed 16 October 2018.
52. See, for example, US Department of Justice, Office of Legal Education, 'Prosecuting Computer Crimes', OLE Litigation Series, 2015, pp. 109–10. As noted in that publication, in the US wire fraud charges under 18 U.S.C. § 1343 carry greater penalties than the cybercrime-specific provisions of 18 U.S.C. § 1030. Furthermore, crimes under 18 U.S.C. § 1343 are predicate offences for the purposes of the Racketeer Influenced and Corrupt Organizations Act (RICO), but crimes under 18 U.S.C. § 1030 are not. For an example of RICO charges brought against alleged cyber-criminals, see US Department of Justice, 'Thirty-Six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes', press release, 7 February 2018, <https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible>, accessed 16 October 2018.
53. CPS, 'Prolific Computer Hacker Jailed for 10 Years'.
54. United Nations Office on Drugs and Crime (UNODC), 'Comprehensive Study on Cybercrime', 2013, p. 16.
55. Verizon, '2018 Data Breach Investigations Report', p. 8.
56. *Ibid.*, p. 5.

to financially motivated cybercrime, most of the available measurements of cybercrime focus on its societal costs[57] rather than criminal revenues.[58]

The revenues from cybercrime are lower than its costs to victims because the latter also encompass the costs of cyber defence, breach mitigation and reputational losses.[59] The assessments of cyber-criminal revenues should be taken with a grain of salt due to methodological challenges and the rapidly evolving nature of cybercrime. For instance, estimates of ransomware revenue covering approximately the same time period range from $25 million in total to $325 million from only one strand of ransomware software.[60]

That said, one commentator assesses the global profits from trading in stolen data at $160 billion, those from selling malware at $1.6 billion, and those from ransomware extortion at $1 billion.[61] One way to cut into those profits and thereby reduce to some extent the economic appeal of cybercrime is through ensuring that money laundering is as difficult and expensive as possible, although the actual effects of this on the incidence of the predicate crime are notoriously difficult to measure.

International Dimension

Cybercrime is global because attacks can be launched from anywhere in the world against a victim in any geographical location. The UK's National Cyber Security Strategy highlights the international character of the threat:

> Much of the most serious cyber crime – mainly fraud, theft and extortion – against the UK continues to be perpetrated predominantly by financially motivated Russian-language organised criminal groups

57. One of the estimates is $600 billion per annum worldwide, calculated by McAfee in 2018. Note that this estimate covers a wide range of crimes outside the scope of this research. See McAfee & Center for Strategic and International Studies (CSIS), 'Economic Impact of Cybercrime – No Slowing Down', February 2018, p. 6.
58. Home Office, 'Understanding the Costs of Cybercrime', pp. 12–21; Ross Anderson et al., 'Measuring the Cost of Cybercrime', 2012, <https://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf>, accessed 16 October 2018.
59. Cabinet Office and Detica, 'The Cost of Cyber Crime', 2011, p. 11, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf>, accessed 16 October 2018.
60. Michael McGuire, 'Into the Web of Profit: An In-Depth Study of Cybercrime, Criminals and Money', Bromium, April 2018, p. 71; see also Europol, *Internet Organised Crime Threat Assessment 2018* (European Cybercrime Centre, 2018), p. 16. The assessment that $325 million was paid in CryptoWall ransoms originates in Cyber Threat Alliance, 'Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat', October 2015. In contrast, a later report by Chainalysis puts global ransomware revenues at $31 million, Chainalysis, 'The Changing Nature of Cryptocrime', January 2018, p. 8.
61. McGuire, 'Into the Web of Profit', p. 43.

> (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries. However, the threat also emanates from other countries and regions, and from inside the UK itself, with emerging threats from South Asia and West Africa of increasing concern.[62]

Some cybercrime, including financially motivated cybercrime, is directly carried out or tolerated by state authorities. The UK and US governments publicly attributed the WannaCry and NotPetya ransomware campaigns in 2017 to the governments of North Korea and Russia, respectively.[63] These attacks were apparently conducted to wreak havoc rather than earn money: for instance, NotPetya damaged files beyond repair when encrypting them.[64] Despite the absence of official attribution, it has been alleged that North Korea was responsible for the financially motivated Bangladesh Bank heist (see Box 3).[65]

If the perpetrators are out of reach due to jurisdictional constraints and the challenges of international cooperation, LEAs may focus on targeting criminal assets or the key nodes of the enabling financial infrastructure, depending on where those are located.[66]

Added Value of Financial Investigation

As mentioned in the Introduction, financial investigation of cybercrime can serve the purposes defined by the FATF. Interviews confirm the usefulness of financial investigation for dealing both with crimes that generate proceeds in cryptocurrency (such as ransomware or cryptocurrency theft) and those that generate proceeds in fiat currency (such as bank account takeover by means of a Trojan infection). There is therefore a strong argument in favour of developing the financial response to cybercrime, in particular by maximising the information input from regulated entities to LEAs and ensuring that regulated entities are aware of LEAs' needs and priorities.

62. HM Government, 'National Cyber Security Strategy 2016-2021', p. 17.
63. White House, 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea', 19 December 2017; Foreign & Commonwealth Office, 'Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks', press release, 19 December 2017, <https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks>, accessed 16 October 2018; NCSC and NCA, 'The Cyber Threat to UK Business: 2017/2018 Report', p. 15.
64. Josh Fruhlinger, 'Petya Ransomware and NotPetya Malware: What You Need to Know Now', *CSO*, 17 October 2017, <https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html>, accessed 16 October 2018.
65. Elias Groll, 'NSA Official Suggests North Korea Was Culprit in Bangladesh Bank Heist', *Foreign Policy*, 21 March 2017; see also the US indictment against a North Korean citizen allegedly taking part in the Bangladesh Bank cyberattack, US vs. Park Jin Hyok, 'Criminal Complaint', US District Court for the Central District of California, MJ18-479, 8 June 2018, paras. 144–87.
66. Author interview with a law enforcement officer, London, May 2018.

Identifying the Scale of Criminality

Financial investigation can be particularly helpful for establishing the true scale of criminality in relation to cryptocurrency crime. For instance, one ransomware attack against a small business, which involved a ransom equivalent to approximately £12,000 at the time, was reportedly linked to a series of other attacks around the world involving more than 25 countries.[67]

In the case of crime that generates proceeds in fiat currency, it is also essential to be able to link related attacks that at first appear to be separate incidents. This is particularly important since connecting a single cyber-criminal group to multiple attacks can prompt LEAs to prioritise the case.[68] In theory, 'following the money' can help make such connections, for instance by tracing the proceeds from several offences to a single bank account. However, unlike in the context of cryptocurrency, the research for this paper did not reveal cases in which this had been achieved in practice. Instead, some financial institutions share information on cyber attacks they face – rather than the resultant financial flows – to make connections between related attacks.[69]

Strategic Disruption

Financial investigation can help identify opportunities for strategic disruption of cyber-criminal operations. For instance, as discussed in Chapter II, money mules are a recurrent feature of money-laundering schemes used in connection to cybercrime. Arresting the people who specialise in recruiting and managing money mules (known as 'mule herders') can therefore introduce a significant disruption to cyber-criminal operations, although identifying and apprehending mule herders remains challenging.[70] This approach has informed the three iterations of the European Money Mule Action coordinated by Europol, the most recent of which led to 159 money mule arrests and the identification of 59 'mule herders' in 2017.[71] Identifying and targeting other money-laundering enablers of cybercrime, such as those that advertise company incorporation for cyber-criminals, can also contribute to disruption.

There are diverging views as to the utility of financial investigation for the purpose of arresting individual money mules. It may provide investigative leads that enable LEAs to trace down the

67. Author telephone interview with a cyber-security academic, March 2018.
68. Author interview with a cyber-security expert, London, April 2018; Michael Levi et al., 'The Implications of Economic Cybercrime for Policing', City of London Corporation, October 2015, pp. 44–45.
69. Author interview with a cyber-security expert, London, April 2018.
70. RUSI workshop on strengthening the anti-money laundering response to cybercrime, London, 30 May 2018.
71. Europol, '159 Arrests and 766 Money Mules Identified in Global Action Week Against Money Muling', press release, 28 November 2017, <https://www.europol.europa.eu/newsroom/news/159-arrests-and-766-money-mules-identified-in-global-action-week-against-money-muling>, accessed 16 October 2018.

'mastermind' cyber-criminal.[72] Unless that happens, going after individual money mules is deemed by some LEAs to have relatively little impact, leading one interviewee to describe this as the 'whack-a-mule' approach.[73]

In contrast, others argue that since the amount one can transfer via a consumer money-mule account is limited, the recruitment of money mules is costly and time consuming in relation to their benefit to the criminal. On that view, closing money-mule accounts can introduce a significant disruption to the operations of cyber-criminals.[74] In any event, both positions recognise the value of dismantling money-mule networks provided that the effect of disruption is sufficiently long lasting.

Providing a Better Intelligence Picture on Cybercrime

In addition to identifying specific disruption opportunities, financial investigation can contribute to developing a general understanding of who cyber-criminals are, where they are located, how they divide their roles and how much they earn.

Cyber-criminals span the range of sophisticated criminal groups to lone actors with limited technical knowledge. Sophisticated cyber-criminal operations typically involve the division of labour between various actors, who often form relatively stable groups but may also rely on third-party service providers for specific tasks.[75] A 2017 report by the NCSC describes the division of labour in organised cyber-criminal groups between a team leader, coders, network administrator, intrusion specialist, data miner, and money specialist.[76] The professionalisation and specialisation of cyber-criminals in their specific areas of expertise is also apparent from an analysis of 27 cyber-criminal networks in the Netherlands.[77] Further insight into the modus operandi of a sophisticated cyber-criminal operation is provided in the US indictment of an alleged cybercrime gang accused of 'captur[ing] the keystrokes of a user on the machine [on]

72. Author interview with a law enforcement officer, London, May 2018.
73. Author interview with a law enforcement officer, London, May 2018 (in reference to the game 'whack-a-mole').
74. Author telephone interview with a law enforcement officer, July 2018.
75. Some outsourced tasks can be very specific, for instance CAPTCHA solving to enable bulk account registrations, see Kurt Thomas et al., 'Framing Dependencies Introduced by Underground Commoditization', Workshop on the Economics of Information Security, 2015.
76. NCSC, 'Cybercrime: Understanding the Online Business Model', pp. 5–6.
77. E Rutger Leukfeldt, Anita Lavorgna and Edward R Kleemans, '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* (Vol. 23, No. 287, 2017), pp. 291–92.

which the keylogger is installed' and thereby gaining access to the victim's bank accounts.[78] The functions of alleged co-conspirators can be summarised as follows:

- A coder who specialised in compromising banking systems.
- Two assistant coders.
- A systems administrator who handled the technical aspects of the scheme.
- A financial manager who was in charge of WebMoney transfers.
- A mule herder in charge of recruiting and managing US-based money mules.
- A mule herder in charge of recruiting and managing UK-based money mules.
- An assistant to the UK-based mule herder.
- Another mule herder.

At the same time, a large number of cyber-criminals are not professional or sophisticated. Many among them are lone actors with limited technical knowledge and cursory planning, especially of the money-laundering stage.[79] Their involvement in cybercrime is facilitated by the CaaS business model.[80] Similarly, the effectiveness and sophistication of their money-laundering techniques (if any) typically depends on the quality of services or advice they can afford online.

Financial investigation can provide insights into the structure, location and modus operandi of both sophisticated cyber-criminal networks and 'lone actor' cyber-criminals that rely on purchasing services from others. Furthermore, it may facilitate filling the knowledge gap regarding the earnings of such rank-and-file cyber-criminals. The gap is in part a function of the difficulty of assessing cyber-criminal revenues, as previously mentioned. For instance, an analysis of 10 Russian-language and three English-language stolen data forums operating from the late 2000s to 2011 has revealed a range of possible aggregate profits made in over 200 transactions, which differ widely depending on the price actually paid to the vendor.[81] That research did not aim to identify profits made by individual criminals. An attempt to do so by another researcher was based on extrapolations from the distribution of revenues among street criminals.[82] Some information is available on the self-reported profits of individuals running stresser services that are used for DDOS attacks. When surveyed by researchers, 'two

78. US vs. Evgeniy Mikhaylovich Bogachev (aka 'LUCKY12345'), 'Criminal Complaint', United States District Court for the District of Nebraska, 4:14MJ3034, 30 May 2014, para. 19.
79. Author telephone interview with a blockchain tracing company, April 2018; author telephone interview with a law enforcement officer, April 2018.
80. NCA, 'Intelligence Assessment: Pathways into Cybercrime', January 2017, p. 4 (focusing specifically on young offenders).
81. Thomas J Holt, Olga Smirnova and Yi-Ting Chua, *Data Thieves in Action: Examining the International Market for Stolen Personal Information* (New York, NY: Palgrave Macmillan, 2016), pp. 58–70.
82. McGuire, 'Into the Web of Profit', pp. 48–53.

participants referred to earning between US$300 to US$500, and US$200 to US$300, per day. Another described it as "easy money"'.[83]

Improved understanding of the earnings of criminals involved in various types of cybercrime is particularly important in view of the potentially misleading impression about the profitability of cybercrime created by spectacular heists that command media attention. The NCSC estimates that 'unless the criminals are able to access large numbers of bulk payment systems, and get high value payouts on each occasion, each individual criminal is relying on small profit margins from each hack just to keep their business going'.[84] Some academic researchers reach similar conclusions, although these are based on research that does not specifically consider the types of cybercrime relevant to this paper.[85] If many cyber-criminals generate low profit margins, even modest increases in the cost of laundering may alter the economic calculus of the profitability of cybercrime.

Expanding Institutional and Legal Capacity

The financial response to cybercrime is becoming increasingly potent thanks to the expanding institutional and legal capacity to use it, as evidenced by at least two developments. One is the increased integration of financial crime and cybercrime expertise within LEAs, and another is a change to EU law requiring cybercrime to be treated as a predicate offence.

Institutional Capacity

In view of the value of financial investigation and growing prevalence of cryptocurrency, both financial investigators and cybercrime units are rapidly acquiring cryptocurrency expertise.[86] This is facilitated by projects such as the one run by N8 Policing Research Partnership in 2017, which developed training and guidance for LEAs based on scenarios of possible criminal use of cryptocurrency.[87] LEAs also engage third-party blockchain analysis companies to work on complex cryptocurrency investigations.[88] In order to strengthen the in-house blockchain analysis

83. Alice Hutchings and Richard Clayton, 'Exploring the Provision of Online Booter Services', *Deviant Behavior* (Vol. 37, No. 10, 2016), pp. 1163, 1172.
84. NCSC, 'Cyber Crime', p. 10.
85. Christin, 'After the Breach', p. 9. The statement relies on two papers (one by Richard Clayton, Tyler Moore and Nicolas Christin; the other by Nektarios Leontiadis) which argue that in most areas of cybercrime a small number of criminals account for the majority of cyber-criminal activity. However, the types of cybercrime considered in those papers do not fall within the scope of the present research, and therefore the extent to which those findings apply is uncertain.
86. Author telephone interview with a law enforcement officer, March 2018.
87. Philip Larratt et al., 'Policing Bitcoin: Investigating, Evidencing and Prosecuting Crimes Involving Cryptocurrency', N8 Policing Research Partnership, 2017, <http://n8prp.org.uk/wp-content/uploads/2017/08/N8-Cryptocurrency-Report.pdf>, accessed 16 October 2018.
88. See, for instance, Europol, 'Europol and Chainalysis Reinforce Their Cooperation in the Fight Against Cybercrime', 19 February 2016.

capacity within LEAs, the EU is funding a project with the participation of Interpol and German and Finnish police that aims to develop additional techniques and tools for analysing blockchain transactions, focusing mostly but not exclusively on Bitcoin.[89]

There are various institutional arrangements for using financial investigation in cybercrime cases involving fiat currency. For example, in the NCA, financial investigation expertise is located within the Intelligence and Operations Directorate and is deployed as a matter of course in support of investigations by the National Cyber Crime Unit (NCCU). However, representatives of other LEAs expressed the view that a greater number of financial investigators would be necessary to maximise the role of financial intelligence in cybercrime investigations.[90]

While there is room for further improvement, the increasing technical ability of LEAs to undertake financial investigations in the domain of cryptocurrency prompts a consideration of how their efforts can be supported by the UK government (for instance, by responding to the risks posed by bitcoin mixers) and regulated entities (for instance, by detecting money-mule accounts), as discussed in Chapter III.

Recognition of Cybercrime as Predicate Offences

In the UK, money-laundering offences under the Proceeds of Crime Act 2002 (POCA 2002) can be committed by handling the proceeds of any criminal offence.[91]

But internationally, neither the UN Convention Against Transnational Organized Crime (UNTOC) nor the FATF's 40 Recommendations require treating cyber-criminal activities as predicate offences.[92] If cyber-criminal activities are not treated as predicate offences, a person who facilitates transactions in property that derives from cybercrime would not be committing a criminal offence, and regulated entities would not be obliged to report such transactions to LEAs. In practice, this is likely to be mitigated by the fact that at least some cyber-criminal activities are likely to fall within the definition of other crimes as well (such as fraud), but unless all cybercrime is adequately covered by definitions of other crimes that constitute predicate offences, a legislative gap will remain.

89. TITANIUM Project, 'FAQ', <https://titanium-project.eu/faq/index.html>, accessed 16 October 2018.
90. Author telephone interviews with two law enforcement officers, March 2018.
91. See the definition of 'criminal property' in section 340(3) and of 'criminal conduct' in section 76 of POCA 2002.
92. UN, 'UN Convention Against Transnational Organized Crime', 2000, Article 6, para. 2b; FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', Interpretive Note to Recommendation 3. The FATF lists categories of crimes that must be designated as predicate offences (see FATF glossary, <http://www.fatf-gafi.org/glossary/d-i/>); cybercrime is not among them; see also UN, 'UN Convention Against Transnational Organized Crime', Article 3, para. 2b; Council of Europe, 'Appendix to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism', 2005.

At the European level, in September 2018 the European Parliament adopted the Directive on Countering Money Laundering by Criminal Law, which requires member states to extend the scope of predicate offences to explicitly cover cybercrime.[93] The rationale behind the Directive is that there remain 'significant differences in the respective definitions of what constitutes money laundering [or] predicate offences'.[94] The legislative change at the EU level shows an increased willingness to tackle the finances of cybercrime. It warrants a consideration of how this ambition can be fulfilled through specific improvements to the existing AML response.

93. European Parliament, 'Legislative Resolution of 12 September 2018 on the Proposal for a Directive of the European Parliament and of the Council on Countering Money Laundering by Criminal Law', Ordinary legislative procedure: first reading (COM(2016)0826 – C8-0534/2016 – 2016/0414(COD), 12 September 2018), Article 2, para. 1v.
94. Council of the European Union, 'Explanatory Memorandum to the Proposal for a Directive of the European Parliament and of the Council on Countering Money Laundering by Criminal Law', *Official Journal of the European Union* (COM/2016/0414(COD)), 21 December 2016.

II. Generation and Laundering of Cyber-Criminal Proceeds

TO UNDERSTAND HOW cyber-criminals launder their proceeds, it is necessary to examine how the proceeds are generated in the first place, and what form they take: cryptocurrency; centralised virtual currency; or fiat currency (in bank accounts or in cash). As discussed in the Introduction, this paper covers activities that involve hacking, malware infections, DDOS attacks or the provision of ancillary services. This chapter breaks down these activities by the type of proceeds and discusses how those proceeds are laundered and used.[95]

Generation of Cyber-Criminal Proceeds

Cyber-criminals can either profit from a cyber attack directly or sell services to other cyber-criminals. If they do profit from an attack directly, the type of attack will determine the form of criminal proceeds. The discussion below summarises the most common ways of generating cyber-criminal proceeds.

Proceeds in Digitally Represented Fiat Currency

Account Takeovers

Modus operandi: Takeovers of customers' accounts with financial institutions mostly take place due to banking malware, including Trojans. Trojans are typically distributed via mass phishing emails or compromised websites. In the case of phishing, a 'mastermind' cyber-criminal – who may or may not have developed the malware – will set up or hire a spam botnet to distribute emails prompting the recipient to download malware disguised as a legitimate file. If a website is involved, the victim will typically either download malware from a compromised webpage, for instance, in response to a notification that they must install a plug-in to reflect multimedia content, or have their log-in data stolen via web-injects, which intercept web traffic to create rogue forms that send the user's input to the criminal.[96] A computer may also be infected without the user purposely downloading any attachment if an 'exploit kit' exploits vulnerabilities

95. Technically, the use of criminal proceeds falls within most definitions of money laundering. For convenience, this chapter treats 'laundering' as disguising or obfuscating the criminal provenance of the proceeds, as distinct from ultimately using them.
96. Secureworks, 'State of Cybercrime 2017: Exposing the Threats, Techniques and Markets That Fuel the Economy of Cybercriminals', 2017, pp. 14–16.

in the user's software to deliver malware.[97] However, Europol's latest Internet Organised Crime Threat Assessment suggests that the use of exploit kits is declining.[98]

Form of proceeds: Since Trojans enable criminals to make unauthorised payments from a user's account with a financial institution, such as a bank or a money-service business (MSB), the proceeds are in digitally represented fiat currency.[99]

Prevalence: Banking Trojans continue to represent a prominent cyber-security threat,[100] although Europol notes that LEAs and cyber-security companies report far fewer instances of infection than they did in the past.[101] That said, a June 2018 report suggests that in the first quarter of 2018 banking Trojans reclaimed from ransomware their position as the most often-used malicious payload in email for the first time since 2016, with Emotet being particularly prominent.[102] Trojans can be either used exclusively by their authors, such as Dridex,[103] or provided as a service, such as Zeus.[104]

Unauthorised Inter-Bank Payments

Modus operandi: While banking Trojans typically entail low-value, high-volume attacks that affect a wide pool of victims in an indiscriminate manner, hacking and malware infections can also be used to execute a number of high-value payments. These are typically carried out by hacking into the SWIFT inter-bank payment system.

Form of proceeds: As with banking Trojans, the proceeds are generated in the form of digitally represented fiat currency in the customer's bank account.

Prevalence: Other than the Bangladesh Bank heist, successful SWIFT attacks include the thefts perpetrated by the Carbanak group against banks in Hong Kong and Ukraine,[105] the hacking of Banco del Austro in Ecuador in 2015,[106] that of Taiwan's Far Eastern International Bank in

97. Holt et al., *Cybercrime and Digital Forensics,* p. 144.
98. Europol, *Internet Organised Crime Threat Assessment 2018,* p. 20.
99. Technically speaking, in these cases, the money in question is a digital representation of a claim vis-à-vis the relevant financial institution.
100. Check Point and Europol, 'Banking Trojans: From Stone Age to Space Era', March 2017, p. 12.
101. Europol, *Internet Organised Crime Threat Assessment 2018,* p. 18.
102. Proofpoint, 'Quarterly Threat Report: Q1 2018', 2018, p. 4.
103. Nikita Slepogin, 'Dridex: A History of Evolution', Securelist, 25 May 2017.
104. 'US vs. Evgeniy Mikhaylovich Bogachev', para. 19.
105. Group-IB, 'Cobalt: Evolution and Joint Operations', May 2018, p. 4.
106. Salvatore Scanio, 'Interbank Liability for Fraudulent Transfers via SWIFT: Banco del Austro, S.A. v. Wells Fargo Bank, N.A.', *Banking & Financial Services Policy Report* (Vol. 36, No. 12, 2017), pp. 8–12.

2017,[107] and that of Banco de Chile in 2018.[108] Although the attackers in some of these cases remain unknown, it has been reported that North Korea's state-run Lazarus Group is responsible for a range of attempted SWIFT intrusions.[109]

Both Bangladesh Bank and Banco del Austro sued their correspondent banks (the New York Fed and Wells Fargo respectively) for honouring the fraudulent instructions, allegedly despite a number of red flags. Banco del Austro has since settled its case and the Bangladesh Bank's lawsuit is pending.[110] In Russia, there have been instances of successful attacks against the country's domestic inter-bank payment system, which was designed as a homegrown alternative to SWIFT,[111] including a theft of $920,000 in July 2018.[112] The NCSC and NCA predict that 'elite' cyber-criminal groups are drifting towards targeted, high-value attacks.[113]

Box 3: Bangladesh Bank Heist

The best-known example of a SWIFT intrusion is the Bangladesh Bank heist of February 2016. The perpetrators surreptitiously installed six types of keylogger malware in the computer system of Bangladesh Bank, the central bank of Bangladesh. This enabled them to send 35 payment orders worth $951 million via SWIFT to the Federal Reserve Bank of New York (New York Fed), where part of Bangladesh Bank's foreign currency holdings was deposited. The SWIFT instructions directed the New York Fed to make payments to a range of recipients. Initially, the New York Fed blocked all 35 requests because they lacked the required formatting but, upon their resubmission by the perpetrators in the correct format, the New York Fed executed five payment requests totalling $101 million while holding up the remaining 30. One of the five transfers, which amounted to $20 million, was soon reversed due to a misspelling in the recipient organisation's name. The remaining $81 million passed through bank accounts opened with fake IDs in the Philippines and was ultimately laundered via casinos.

Sources: NCSC and NCA, 'The Cyber Threat to UK Business: 2016/2017 Report', p. 12; Daniel Bentley, 'The New York Fed Came This Close to Stopping the $81 Million Cyber Bank Heist', Fortune, *6 June 2016; Victor Mallet and Avantika Chilkoti, 'How Cyber-Criminals Targeted Almost $1bn in Bangladesh Bank Heist',* Financial Times, *18 March 2016.*

107. NCSC and NCA, 'The Cyber Threat to UK Businesses: 2016/2017 Report', p. 20.
108. Jeremy Kirk, 'Banco de Chile Loses $10 Million in SWIFT-Related Attack', *Bank Info Security*, 13 June 2018.
109. McAfee & CSIS, *Economic Impact of Cybercrime,* p. 10; see also Danny Palmer, 'New Wave of Cyberattacks Against Global Banks Linked to Lazarus Cybercrime Group', *ZD Net,* 13 February 2017.
110. Jonathan Spicer and Ruma Paul, 'Bangladesh Eyes Settlement in U.S. Cyber Heist Suit Ahead of its Own Case', *Reuters,* 16 April 2018.
111. Group-IB, 'MoneyTaker: 1.5 Years of Silent Operations', December 2017.
112. Catalin Cimpanu, 'Hackers Breach Russian Bank and Steal $1 Million Due to Outdated Router', *Bleeping Computer*, 19 July 2018.
113. NCSC and NCA, 'The Cyber Threat to UK Business: 2017/2018 Report', p. 21.

Proceeds in Cash

Hacking of ATMs and Card Processing

Modus operandi: Hacking ATMs – also known as 'logical attacks' or 'jackpotting' – and card-processing attacks are noteworthy for generating proceeds in cash. ATM hacking can be done by means of either connecting a physical information drive (such as a USB) to an ATM to upload malware, or connecting a skimming device to it (a physical attack), or intruding in the bank's internal network and remotely directing the ATM to dispense cash (a network attack).[114] A separate type of attack – attacks on card-processing systems – involves removing cash withdrawal and overdraft limits on selected credit or debit cards.[115]

Form of proceeds: The proceeds are collected in cash from numerous ATMs. As a consequence, large-scale ATM hacking or card-processing attacks require the engagement of a significant number of money mules. For instance, a failed attempt to steal more than €25 million from a bank in Central Europe by the Cobalt group would have reportedly involved over a hundred money mules.[116] From a money mule's perspective, ATM hacking entails greater risks of detection because it requires collecting money from a specific ATM at a given time.[117]

Prevalence: Since ATM malware was first observed in Eastern Europe in 2009, instances of physical ATM attacks have been observed across Europe, Southeast Asia and North America.[118] The requisite malware can be purchased on the Dark Web.[119] Although few criminal groups are able to launch a successful network intrusion,[120] the Carbanak/Cobalt case suggests that the risk is real.

114. Trend Micro and Europol, 'Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types', 2017.
115. Group-IB, 'MoneyTaker', p. 26.
116. Author telephone interview with a cyber-security expert, June 2018.
117. Group-IB, 'MoneyTaker', p. 26.
118. Trend Micro and Europol, 'Cashing in on ATM Malware', pp. 30–33; Brian Krebs, 'First "Jackpotting" Attacks Hit U.S. ATMs', *Krebs on Security*, 28 January 2018.
119. Trend Micro and Europol, 'Cashing in on ATM Malware', p. 33.
120. *Ibid*.

Box 4: Carbanak/Cobalt Attacks

The Carbanak Trojan – known initially as Anunak – was developed in 2013 and successfully used by the perpetrators in 2014. Attacks throughout 2014 overwhelmingly targeted Russia but diversified to encompass Germany and the US by early 2015. Unlike other contemporary Trojans, Carbanak targeted banks directly rather than their customers. Its distribution relied on phishing emails.

Infecting banks with Carbanak gave the perpetrators control over the bank's payment-processing systems and/or ATMs. They could therefore:

- Make payments to bank accounts owned by companies they had created.
- Force ATMs to spit out cash that money mules would pick up.
- Deactivate cash withdrawals and overdraft limits to enable cash withdrawals by money mules.

In 2016, the group further refined its modus operandi. Average losses per bank amounted to $2 million. In total, Europol assesses 'cumulative losses' from Carbanak/Cobalt for the financial industry at €1 billion, although it is not entirely certain whether this figure is only meant to reflect the profit earned by the criminals or mitigation costs as well. The money-laundering techniques used depended on the amount misappropriated. Amounts up to $3 million reportedly passed through a network of companies on to credit card accounts of individual money mules. Larger amounts were laundered through corporate accounts. The perpetrators also reportedly used digital payment providers such as WebMoney, Yandex Money and Qiwi, as well as at least five money-mule networks.

The alleged leader of the group was arrested in Spain in March 2018. The criminal conspiracy unravelled once Taiwanese police managed to apprehend two money mules. The analysis of communications data on their mobile phones led the investigators to the alleged leader of the criminal group. However, Cobalt attacks continued, albeit on a reduced scale, even after the arrest.

Sources: Alex Drozhzhin, 'The Greatest Heist of the Century: Hackers Stole $1 Bln', Kaspersky Daily, *16 February 2015; Kaspersky Lab, 'Carbanak APT: The Great Bank Robbery', February 2015, pp. 17–18; Group-IB and Fox-IT, 'Anunak: APT Against Financial Institutions', December 2014, p. 2; Brian Krebs, 'The Great Bank Heist, or Death by 1,000 Cuts?', Krebs on Security, 16 February 2015; Pavel Sedakov and Dmitriy Fionov, 'Brat' Po-Krupnomu: Odna Gruppirovka Khakerov Ograbila Bolee 50 Bankov' ['Playing it Big: One Hacker Group Robbed Over 50 Banks'],* Forbes Russia, *22 December 2014, <http://www.forbes.ru/tekhnologii/internet-i-svyaz/276227-brat-po-krupnomu-kak-odna-gruppirovka-khakerov-ograbila-bolee-50>, accessed 16 October 2018; Group-IB and Fox-IT, 'Anunak', pp. 2, 10–11, 21–22; Europol, 'Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain', press release, 26 March 2018, <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>, accessed 16 October 2018; Europol and Trend Micro, 'Cashing in on ATM Malware'; Charlie Devereux, Franz Wild and Edward Robinson, 'The Biggest Digital Heist in History Isn't Over Yet',* Bloomberg, *25 June 2018; Group-IB, 'Cobalt: Evolution and Joint Operations', May 2018, p. 15.*

Proceeds Mostly in Cryptocurrency

Payments from Other Criminals

Modus operandi: Cybercrime is enabled by a vibrant underground economy. Illegal products and services are typically sold on Dark Web marketplaces, but also occasionally on the surface web. Dark Web marketplaces offer a wide array of items ranging from drugs to child pornography to digital products, such as malware kits, stolen data, hacking for hire or money-laundering services. Despite the law enforcement takedown of three major Dark Web marketplaces in 2017, a number of smaller marketplaces remain in operation, while higher-skilled cyber-criminals operate their own websites to sell services.[121]

Form of proceeds – Dark Web: Cryptocurrency is the preferred payment medium on the Dark Web, although WebMoney continues to be used from time to time.[122] Earlier research refers to E-Gold, Liberty Reserve and Yandex Money, which were historically in use on Dark Web marketplaces, although the former two are now defunct due to law enforcement interventions.[123] Bitcoin remains by far the most popular cryptocurrency, including for transactions among criminals.[124] This is so despite the indications that Dark Web marketplaces are increasingly accepting the privacy coin Monero due to its reduced traceability.[125] In addition to bitcoin's first-mover advantage, its prevalence is likely to be due to its relatively high liquidity and easy convertibility into fiat currencies. In contrast, Monero ordinarily needs to be converted into bitcoin before it can be transferred into fiat currency.[126] An analysis of 150 Dark Web message boards conducted by Recorded Future suggests that in fact it is Litecoin – another cryptocurrency with a transparent blockchain – that is the second most popular cryptocurrency among criminals after bitcoin, with privacy-focused Dash coming third.[127] Some of the possible explanations for

121. Europol, *Internet Organised Crime Threat Assessment 2018*, p. 48.
122. Author interview with a law enforcement officer, London, May 2018. Literature suggests centralised virtual currencies are at present mostly used by Eastern European cyber-criminals; see Goncharov, 'Criminal Hideouts for Lease', p. 15; Benjamin Brown, '2016 State of the Dark Web', *Akamai*, 2016, p. 6.
123. Alice Hutchings and Thomas J Holt, 'A Crime Script Analysis of the Online Stolen Data Market', *British Journal of Criminology* (Vol. 55, No. 3, 2015), pp. 596, 606.
124. Author telephone interview with a law enforcement officer, February 2018; Europol, *Internet Organised Crime Threat Assessment 2017* (European Cybercrime Centre, 2017), pp. 11, 13, 56, 61; Andrei Barysevich and Alexandr Solad, 'Litecoin Emerges as the Next Dominant Dark Web Currency', *Recorded Future Blog*, 8 February 2018; Robert Novy, remarks at the hearing entitled 'Illicit Use of Virtual Currency and the Law Enforcement Response', US House of Representatives, Financial Services Committee, 20 June 2018; Trend Micro, 'U-Markt: Peering into the German Cybercriminal Underground', 2015, pp. 14–16, 21.
125. Chainalysis, 'The Changing Nature of Cryptocrime', January 2018, p. 8.
126. Author interview with an AML expert, London, March 2018.
127. Barysevich and Solad, 'Litecoin Emerges as the Next Dominant Dark Web Currency'.

Litecoin's apparent popularity include transaction speed (four times faster than bitcoin) and the fact that it is one of the oldest and therefore most familiar cryptocurrencies.[128]

Form of proceeds – paying for DDOS: In addition to payment methods accepted on Dark Web marketplaces, fiat currency is frequently used to pay for DDOS attacks that are ordered from stresser websites on the surface web.[129] The operators of such websites often accept payments via legitimate payment service providers, such as PayPal, or credit cards.[130] Some of their clientele lack the sophistication to realise the detection risks associated with paying from their own accounts; others use stolen PayPal accounts or credit cards.[131] A survey by academic researchers of individuals running DDOS stressers highlights how limiting the availability of reliable payment methods affects the business model of such websites:

> The most disruption reported by participants in the operation of their services was in relation to payment methods, with seven participants advising that these had changed over time. Of these, six had trouble accepting payments through PayPal, the preferred payment method. For example: 'Paypal is always closing us down for running stressers, it's really a problem as that is our main way to get paid.' … Another participant advised that his payment methods had changed when Liberty Reserve had been shut down, and that he had recently begun accepting credit cards and digital currencies.[132]

Those criminals that accept credit card payments need to set up a company and a corporate bank account to receive the funds. They therefore pose as legitimate merchants and often set up fake websites to deceive the acquiring bank (as well as any other bank whose services they may use) as to the nature of their business.

Prevalence: Trading in stolen data is especially widespread.[133] Mass data breaches, such as the theft of credit card data of more than 41 million customers of the US retail company Target, mean that criminals have more information than they can use, which creates incentives to sell it.[134]

Extortion from the Victim

Modus operandi: Extortion often involves ransomware or DDOS attacks. Ransomware attacks entail the demand of a ransom for decrypting the files encrypted by ransomware malware. DDOS victims are required to pay to avoid having their website taken down by a DDOS attack, which

128. The authors are grateful to one of the peer reviewers for their insight on this.
129. See, for example, NCSC and NCA, 'The Cyber Threat to UK Business: 2016/2017 Report', p. 6; Europol, 'Joint International Operation Targets Young Users of DDOS Cyber-Attack Tools'.
130. Catalin Cimpanu, '34 Users Who Paid for DDoS Attacks Arrested by Police, 101 More Questioned', *Bleeping Computer*, 12 December 2016; Hutchings and Clayton, 'Exploring the Provision of Online Booter Services', p. 1163.
131. Author telephone interview with a law enforcement officer, April 2018.
132. Hutchings and Clayton, 'Exploring the Provision of Online Booter Services'.
133. McGuire, 'Into the Web of Profit', pp. 64–67.
134. Holt et al., *Data Thieves in Action,* pp. 1–3.

can be highly disruptive for business. However, in some cases extortion can involve the threat of releasing stolen information to the public, as when hackers demanded $1 million worth in Ripple (XRP) from the Bank of Montreal and Simplii Financial.[135] Unlike DDOS attacks that target specific victims, ransomware attacks used to be undirected and often demanded the same amount of ransom regardless of whether the victim was a small company or a multibillion dollar business,[136] but there has been a recent trend towards more focused ransomware attacks.[137]

Form of proceeds: The emergence of cryptocurrency has been essential to the spread of ransomware and DDOS extortion because it provides a pseudonymous payment medium (in other words, users need not disclose their identity to make or receive payments) that does not require the involvement of intermediaries such as banks, which conduct customer due diligence (CDD) and report suspicious activities.[138] Currently, ransoms are overwhelmingly paid in cryptocurrency, especially bitcoin.[139] This example shows how the availability of the necessary financial infrastructure can affect the magnitude of a given type of cybercrime.

There is also evidence of cyber-criminals involved in extortion increasingly resorting to Monero, a privacy-focused coin that renders transaction tracing extremely difficult.[140] Despite the overwhelming prevalence of cryptocurrency, there are isolated instances of ransomware attacks accepting ransom in WebMoney or Perfect Money.[141]

Prevalence: The UK's NCSC and NCA identified ransomware extortion and DDOS attacks as one of the prominent trends of 2017, citing among other things the payment by a South Korean web-hosting company of $1 million in bitcoin as ransom to avert a DDOS attack.[142] Later estimates suggest that, as of early 2018, DDOS attacks continued to increase in number and intensity.[143]

---

135. *Finextra*, 'BMO and Simplii Hackers Demand Ransom of $1m in XRP', 30 May 2018.
136. Author telephone interview with a cyber security expert, March 2018.
137. Author telephone interview with a law enforcement officer, February 2018.
138. Author telephone interview with a law enforcement officer, February 2018; author interview with an AML expert, London, March 2018; author telephone interview with a cyber-security academic, March 2018; Novy, remarks at the hearing entitled 'Illicit Use of Virtual Currency and the Law Enforcement Response'.
139. Europol, *Internet Organised Crime Threat Assessment 2016* (European Cybercrime Centre, 2016), p. 11; author telephone interview with a cyber forensic expert, March 2018; author telephone interview with an international organisation representative, March 2018.
140. See, for example, Kevin Townsend, 'Largest Ever 1.3Tbps DDoS Attack Includes Embedded Ransom Demands', *Security Week*, 5 March 2018.
141. Tal Pavel, 'Ransomware Named Tyrant Attacking Computers in Iran', *Jerusalem Post,* 30 October 2017; Lawrence Abrams, 'New LLTP Ransomware Appears to be a Rewritten Venus Locker', *Bleeping Computer,* 21 March 2017.
142. NCSC and NCA, 'The Cyber Threat to UK Business: 2017/2018 Report', p. 7.
143. Verisign, 'Distributed Denial of Service Trends Report', Volume 5, Issue 1 – 1st Quarter, 2018, p. 4.

Proceeds in Cryptocurrency

Cryptocurrency Theft

Modus operandi: The proliferation of cryptocurrency exchanges has led to a series of attacks resulting in the theft of cryptocurrency. Although attacks can also be directed against individual users, more ambitious criminals target cryptocurrency exchanges or custodian wallets, which hold cryptocurrency on behalf of a large number of users.

Form of proceeds: Like ransomware and trading on the Dark Web, these crimes directly generate proceeds in cryptocurrency, with the important difference that they involve large amounts of funds obtained from a single source in a short period of time.

Prevalence: Among the best-known victims is Mt. Gox, the world's largest bitcoin exchange at the time when it lost 660,000 bitcoins (equivalent to $7.5 million then and almost $3.0 billion in November 2018 prices) to a series of cyber intrusions between September 2011 and July 2013.[144] The scale of cryptocurrency theft then continued to grow and increased seven-fold between 2015 and 2016 alone.[145] In January 2018, $550 million of NEM coins was stolen from the Japanese exchange Coincheck,[146] contributing to the total of $927 million of cryptocurrency stolen in the first three quarters of 2018.[147] It has also been reported that malware for stealing cryptocurrency from bitcoin ATMs[148] is available on the Dark Web.[149]

Cryptojacking

Modus operandi: Alongside cryptocurrency theft, surreptitiously using another person's device to mine[150] cryptocurrency for the criminal's benefit is another high-growth area of cybercrime that generates proceeds in cryptocurrency. Criminal cryptojacking involves installing malware on a victim's computer, which is typically seen as a form of illegal hacking. In contrast, in-browser cryptojacking involves placing a JavaScript that makes the users of a website mine cryptocurrency for the benefit of the website's operator. The latter form of cryptojacking may be seen as a legitimate alternative to relying on advertising for revenue. According to a recent report, a suspect in a Japanese cryptojacking case argued that the software he used was 'not a virus [but] a software script that brings monetization similar to online ad distribution

144. Chainalysis, 'The Changing Nature of Cryptocrime', p. 6.
145. *Ibid*.
146. *Fortune*, 'How to Steal $500 Million in Cryptocurrency', 31 January 2018.
147. CipherTrace, 'Cryptocurrency Anti-Money Laundering Report', Q3, 2018, p. 9.
148. A physical kiosk connected to the internet and providing cryptocurrency exchange services.
149. Charlie Osborne, 'You Can Buy Bitcoin ATM Malware for $25,000 in the Dark Web', *ZD Net*, 8 August 2018.
150. That is, solve a cryptographic puzzle that is used for validating transactions on the blockchain. Users who solve the puzzle are rewarded with new coins.

platforms'.[151] However, there are also known instances of criminals hacking other people's websites to install cryptojacking JavaScript codes.[152] According to Europol, the pro-Daesh (also known as the Islamic State of Iraq and Syria, ISIS) website Akhbar al-Muslimin contained an embedded cryptojacking code.[153]

It has been suggested that cryptojacking is easier to monetise than ransomware because it does not rely on the victim making a payment.[154] Moreover, since even criminal cryptojacking causes no immediately visible damage to victims, it is more difficult to detect than other types of malware.[155]

Form of proceeds: Cryptojacking mostly aims at mining Monero rather than bitcoin, otherwise a more widespread cryptocurrency. This is because Monero mining uses ordinary central processing units (CPUs) while bitcoins can now only effectively be mined using specialised hardware (application-specific integrated circuits).[156]

Prevalence: The incidence of cryptojacking malware reportedly grew by 629% between late 2017 and June 2018.[157] The NCA assesses that cryptojacking malware infected 1.65 million computers worldwide in the first nine months of 2017.[158]

Purchasing Goods

Card Cloning, Chip Compromise and Carding

Modus operandi: Since mass data breaches generate more stolen credit card data than one criminal can use, the ability to sell stolen data to others is essential to the profitability of hacking. Although the ultimate use of cards for purchases can be seen as a type of cyber-enabled fraud, it is inextricably linked to the original cybercrime that led to the theft of the card information.[159]

151. *CCN*, 'Monero Miners to See Charges in Japan's First CryptoJacking Criminal Case', 13 June 2018.
152. Europol, *Internet Organised Crime Threat Assessment 2018*, p. 19.
153. *Ibid.*, p. 53.
154. McAfee, 'McAfee Labs Threats Report', June 2018, p. 6.
155. *Ibid.,* p. 12.
156. Shayan Eskandari et al., 'A First Look at Browser-Based Cryptojacking', paper presented at the IEEE Security & Privacy on the Blockchain Workshop, London, 23 April 2018; Richard Clayton, 'Dave Jevans's Presentation at the Cambridge Cybercrime Centre's Third Annual Cybercrime Conference', liveblogged, *Light Blue Touchpaper,* 12 July 2018, <https://www.lightbluetouchpaper.org/2018/07/12/cybercrime-conference/>, accessed 16 October 2018.
157. McAfee, 'McAfee Labs Threats Report', pp. 2, 6.
158. NCA, 'National Strategic Assessment of Serious and Organised Crime 2018', May 2018, para. 262.
159. See David Wall, 'How Big Data Feeds Big Crime', *Current History* (Vol. 117, No. 795, 2018), pp. 29, 30–31.

Two major types of stolen credit card data include '"dumps" (the data copied from the magnetic strip of a card) and "CVVs" (the data required to make an online or telephone card purchase)'.[160]

Form of proceeds: 'Dumps' enable cyber-criminals to clone a card and use it for offline purchases in brick-and-mortar merchant shops, as opposed to online marketplaces.[161] In that case, cyber-criminals do not need to rely on reshipment mules to order the goods on their behalf. In many countries, the potential for fraud using dumps has been addressed by using Europay, MasterCard, Visa (EMV) chips instead of magnetic cards. The use of EMV chips generates unique codes at the point of sale so that the compromise of any particular point of sale does not enable the criminal to reverse engineer the card and use it elsewhere. Since EMV was introduced in the UK in 2004, card fraud has declined by 71%.[162] The US has moved towards using EMV in the past several years.[163] Despite the additional security that EMV offers, criminals have occasionally found ways to compromise EMV chips and therefore make unauthorised purchases.[164]

The card verification value (CVV2) code is printed on the back of a card and is needed for online purchases.[165] A wide variety of goods can be purchased online through the use of CVV2 data, including, for instance, airline tickets.[166] Dumps are reportedly worth more than the CVV2 data because purchasing goods in brick-and-mortar shops using cloned cards is considered easier than ordering goods online, since the latter requires a delivery address and therefore leaves a trail.[167]

Prevalence: As mentioned in the discussion of payments from other criminals, the trade in and misuse of stolen data, including credit card information, is widespread and facilitated by a number of specialised websites, including those on the surface web.[168]

Summary

Table 2 summarises the most common techniques of generating cyber-criminal proceeds described in the preceding part of this chapter.

160. Europol, *Internet Organised Crime Threat Assessment 2017*, p. 50.
161. Brian Krebs, 'All About Fraud: How Crooks Get the CVV', *Krebs on Security*, 26 April 2016.
162. Financial Fraud Action UK, 'Annual Review 2017', p. 13.
163. Windsor Holden, 'Payment Trends in the US – The EMV Migration and the Future of Mobile Payments', *The Paypers,* 24 January 2018.
164. Brian Krebs, 'Secret Service Warns of Chip Card Scheme', *Krebs on Security*, 5 April 2018.
165. *Ibid.*
166. Alice Hutchings, 'Leaving on a Jet Plane: The Trade in Fraudulently Obtained Airline Tickets', *Crime, Law and Social Change* (8 May 2018), doi:10.1007/s10611-018-9777-8.
167. Krebs, 'All About Fraud'.
168. Europol, *Internet Organised Crime Threat Assessment 2017*, p. 50. See also Max Goncharov, 'Russian Underground 2.0', Trend Micro, July 2015, pp. 21–25; Alexander Mikhaylov and Richard Frank, 'Cards, Money and Two Hacking Forums: An Analysis of Online Money Laundering Schemes', paper presented to the 2016 European Intelligence and Security Informatics Conference, Uppsala, Sweden, 17–19 August 2016.

Table 2: Most Common Techniques of Generating Cyber-Criminal Proceeds

Type of Activity / Source of Proceeds	Hacking/Malware	DDOS Attacks	Ancillary Services
Crimes that generate proceeds in digitally represented fiat currency			
Account takeovers	Fiat currency: in an account with a financial institution		
Unauthorised inter-bank payments	Fiat currency: in a bank account		
Crimes that generate proceeds in cash			
Hacking of ATMs	Fiat currency: cash		
Card-processing attacks	Fiat currency: cash		
Crimes that mostly generate proceeds in cryptocurrency			
Receiving payment from other criminals	Virtual currency: • Cryptocurrency • Centralised virtual currency Fiat currency: • Via online payment providers (using personal or stolen accounts) • Via bank transfer (payments most likely to involve stolen credit card details or to originate from less sophisticated purchasers) • Via mobile payment services • Via prepaid cards		
Extortion from the victim	Virtual currency: • Cryptocurrency • Centralised virtual currency		
Crimes that generate proceeds in cryptocurrency			
Cryptocurrency theft	Cryptocurrency		
Cryptojacking	Cryptocurrency		
Crimes that involve purchasing goods			
Card cloning or chip compromise	Goods purchased from bricks-and-mortar merchants		
Carding	Goods purchased from online merchants		

Sources: The authors , 2018; Cedric Pernet, 'The French Underground: Under a Shroud of Extreme Caution', Trend Micro, 2016, pp. 10, 17. Research interviews for this paper provided no evidence of extortion demands to pay in fiat currency, whether in the context of ransomware or DDOS attacks. However, such demands

could conceivably be made. This activity is therefore placed among crimes that mostly generate proceeds in cryptocurrency in this table.

Money-Laundering Techniques

This section discusses typical money-laundering techniques used by cyber-criminals. It begins by looking at the cross-cutting difference between laundering the proceeds of high-value, low-volume (targeted) attacks and those of low-value, high-volume (indiscriminate) attacks. It then discusses typical money-laundering techniques that exploit the following: the financial sector; the cryptocurrency infrastructure; and e-commerce, e-gambling and online gaming outlets.

Depending on its complexity, a money-laundering scheme can span several sectors and involve, for example, both bank transactions and cryptocurrency transfers. However, the form of the proceeds sometimes dictates the use of a particular laundering technique. For instance, the proceeds of cryptocurrency theft will inevitably be laundered through cryptocurrency transactions aimed at obscuring the criminal origin of the coins.

High-Value, Low-Volume Versus Low-Value, High-Volume Attacks

The distinction between high-value, low-volume (targeted) attacks and low-value, high-volume (indiscriminate) attacks cuts across several types of cybercrime. The former generate large amounts of funds from a single victim. The latter involve smaller payments from a large pool of victims, although they can amount to significant sums in the aggregate. These two types of attacks require a different approach to money laundering.[169]

The distinction is especially significant in the context of attacks against financial institutions and their customers. As discussed near the beginning of Chapter II, unauthorised inter-bank transfers are typically caused by an intrusion in the SWIFT payment system and involve millions of dollars. In contrast, banking Trojans normally infect bank customers' computers and lead to withdrawals of more modest amounts from the accounts of a large pool of victims. While the latter can be channelled through consumer accounts without triggering bank alerts, this is not the case with large amounts of funds, which therefore require corporate accounts and an ostensibly legitimate business purpose for the payment.

The distinction between high-value and low-value attacks can also be drawn between ransomware on the one hand and theft from cryptocurrency exchanges on the other. Although the set of money-laundering techniques used by the criminals remains essentially the same in this context, it is easier for LEAs and private blockchain analysis companies to detect tainted cryptocurrency from large-scale attacks.[170] Besides, if coins based on a transparent blockchain

169. Author interview with a bank, London, March 2018; author telephone interview with a financial consultancy firm, March 2018.

170. See, for example, John Bohannon, 'Why Criminals Can't Hide Behind Bitcoin', *Science Magazine*, 9 March 2016.

are stolen, a hacked exchange will normally know exactly what coins have gone missing and to which address they have been diverted. For these reasons, it was argued that a major difficulty faced by the perpetrators of the Coincheck hack would be converting stolen NEM coins into fiat currency.[171] In the end, however, the coins were exchanged for bitcoin and Litecoin at a 15% discount via a peer-to-peer Dark Web exchange set up by the hackers themselves.[172]

Financial Sector

Financial institutions can play the dual role of potential victim of cybercrime as well as its unwitting financial facilitator. The long-standing preoccupation of financial institutions has been ensuring their own and their customers' security against cyber threats. In view of the significant amounts generated by cybercrime, this approach is being increasingly complemented by a focus on cybercrime as a source of illicit proceeds and therefore an AML challenge.

Money-Mule Accounts

A prevalent money-laundering threat related to cybercrime is money-mule accounts. According to Europol, over 90% of money-mule transactions are cybercrime-related, although this estimate also covers cyber-enabled fraud such as 'romance scams'.[173] Depending on the context, the term 'money mule' can refer to:

- A person who receives funds in their bank account and transfers them to a cyber-criminal.
- A person who sells control over their bank account to a cyber-criminal.
- A person who opens a bank account for the benefit of a cyber-criminal using a fake ID.
- A person whose bank account has been taken over by a cyber-criminal.
- A person who picks up cash from ATM hackings or card-processing attacks.
- A person who reships goods that have been purchased by a cyber-criminal using stolen credit card details.

In some of these scenarios, it is preferable to speak of a 'money-mule account' rather than a money mule: the owner of a compromised bank account is not responsible for the transfer of funds that a criminal may direct through their account. Money-mule accounts can also be opened with the help of corrupt bank insiders.[174] Those money mules who are recruited to carry out tasks on behalf of a cyber-criminal can be anywhere on a spectrum between innocent ignorance and complicity.[175]

---

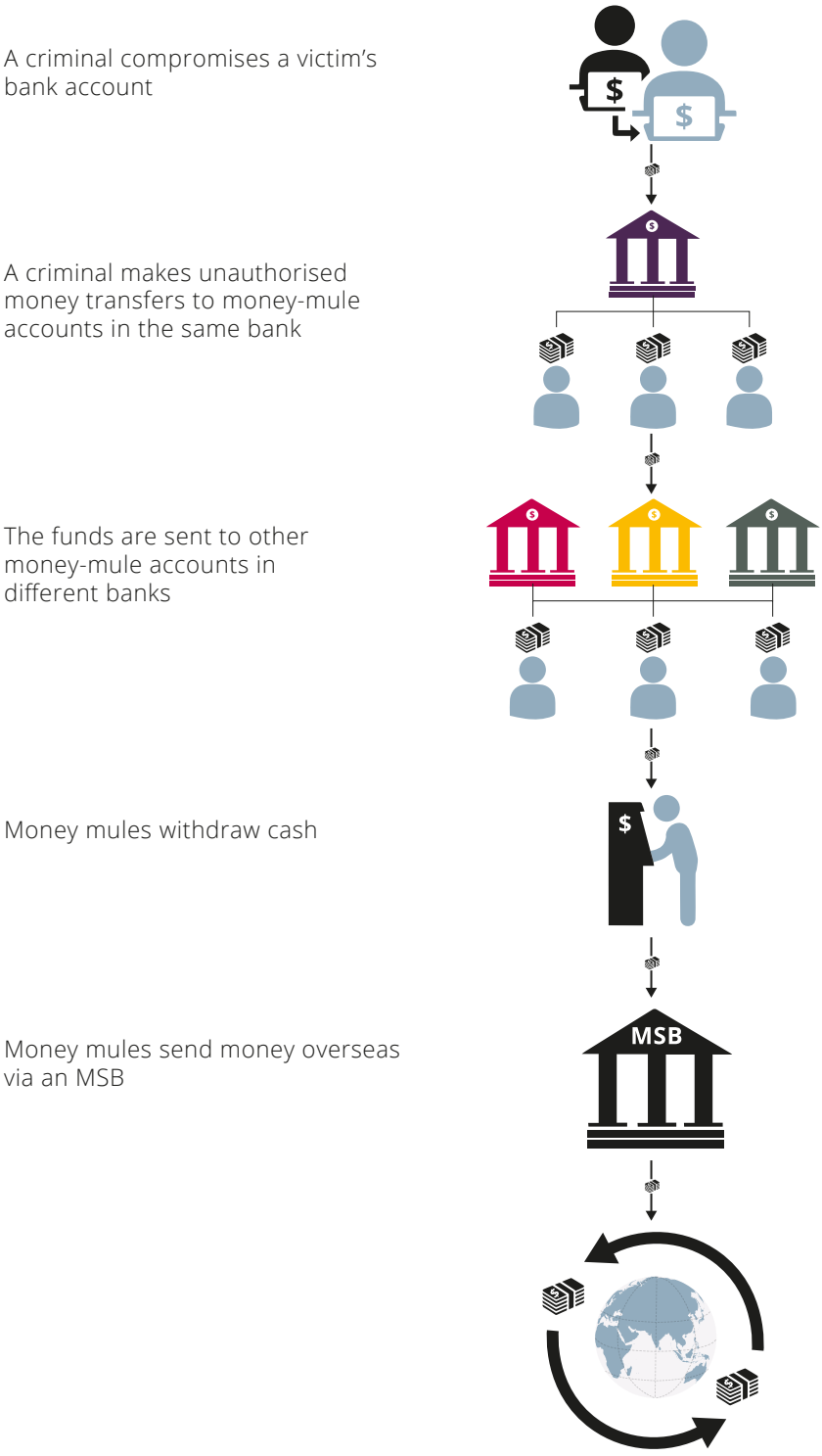
171. *Fortune,* 'How to Steal $500 Million in Cryptocurrency'.
172. Jonathan Foster, 'Coincheck Hackers Have Laundered All of Their NEM', *Deep Dot Web*, 9 April 2018.
173. Europol, 'Money Muling: Public Awareness and Prevention', <https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling>, accessed 16 October 2018.
174. NCA, 'Bank Employee Abused Position to Launder Millions', 13 December 2017.
175. Rainer Hulsse, 'The Money Mule: Its Discursive Construction and the Implications', *Vanderbildt Journal of Transnational Law* (Vol. 50, No. 1007, 2017), pp. 1014–15.

The use of money-mule accounts is particularly common in account takeover cases. After compromising a victim's account, a criminal will typically make an unauthorised money transfer to a money-mule account, followed by transfers via several more money-mule accounts. The first several transfers sometimes take place between accounts within the victim's bank to ensure instantaneous processing of payments.[176] The number of money-mule accounts, banks and jurisdictions involved depends on the complexity of the scheme.[177]

In the end, it is typical for a money mule to withdraw cash and transfer it overseas via an MSB. This last step is intended to 'break the link between the crime and the proceeds'.[178] A wide variety of MSBs are used, with the largest ones being particularly exposed to this risk because of their size.[179] Jurisdictions cited by interviewees as common destinations for funds stolen in the UK include Hong Kong, mainland China, Gulf countries and Eastern Europe.[180]

176. Check Point and Europol, 'Banking Trojans', p. 13; author interview with a law enforcement officer, March 2018.
177. Cellule de Traitement des Informations Financières (Belgian Financial Intelligence Processing Unit), '24e rapport d'activités', 2017, p. 26.
178. Europol, *Why Is Cash Still King? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering* (The Hague: Europol Police Office, 2015), p. 10. See also Eurasia Group on Combating Money Laundering and Financing Terrorism (EAG), 'Typology Project: Cybercrime and Money Laundering', 2014, p. 32.
179. Hulsse, 'The Money Mule', p. 1017.
180. Author interview with a law enforcement officer, London, March 2018; author interview with a law enforcement officer, London, May 2018.

Figure 1: Basic Steps in Laundering the Proceeds of an Account Takeover



Source: The authors, 2018.

The use of money mules recruited by cyber-criminals to perform various tasks is geographically ubiquitous, from the EU[181] to the Western Balkans[182] to the US[183] to Asia-Pacific.[184] While some cyber-criminal groups, such as the Cobalt group,[185] cultivate their own money-mule networks, others rent the services of third-party networks. Outsourcing entails additional costs but alleviates the group's dependence on its money mules and buttresses its resilience against law enforcement interventions.[186] Such third-party money-mule networks facilitate a wide array of crime, not only cybercrime.[187]

Corporate Accounts

In addition to individual accounts, cyber-criminals also use companies and corporate accounts for money laundering, especially if larger amounts are involved.[188] In one case, a group of Ukrainian hackers set up a front company to recruit – and, presumably, pay – other hackers under the guise of legitimate employment.[189]

There is therefore reportedly an overlap between money-laundering techniques used for cybercrime and what is often considered 'high-end money-laundering' techniques.[190] Companies incorporated in Germany, the UK and the US have been reported to be especially popular on Russian Dark Web markets, where the going rate for incorporation services is $50,000.[191] According to one interviewee, little is known about the identities of enablers who incorporate companies for cyber-criminals and whether (some of) these are the same individuals who facilitate high-end money laundering in other contexts.[192] Given the rise in prevalence of SWIFT intrusions in the past three years, more analysis is necessary in relation to how and where

181. Europol, '159 Arrests and 766 Money Mules Identified in Global Action Week Against Money Muling'.
182. Author telephone interview with an international organisation representative, March 2018.
183. As in the case of laundering the proceeds of Dridex/Bugat, see US vs. Andrey Ghinkul, 'Amended Preliminary Injunction', United States District Court for the Western District of Pennsylvania, 15-198, 16 September 2015, paras. 27–36.
184. Author Skype interview with an AML expert, April 2018.
185. BAE Systems, *Threat Intelligence, Cobalt Gang Mules?,* 16 May 2018, p. 1.
186. Author interview with a law enforcement officer, London, May 2018.
187. Author conversation with a law enforcement officer, London, July 2018; Leukfeldt et al., 'Organised Cybercrime or Cybercrime that is Organised?', p. 291.
188. Belgian FIU, '24e rapport d'activités', p. 26.
189. US Department of Justice, 'Three Members of Notorious International Cybercrime Group "Fin7" In Custody for Role in Attacking Over 100 U.S. Companies', press release, 1 August 2018, <https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100>, accessed 16 October 2018.
190. Author interview with a law enforcement officer, London, May 2018; on high-end money laundering, see NCA, 'High End Money Laundering Strategy and Action Plan', December 2014.
191. Goncharov, 'Russian Underground 2.0', p. 11.
192. Author interview with a law enforcement officer, London, May 2018.

cyber-criminals set up companies and open corporate bank accounts. In particular, the potential role that professional advisers such as lawyers, accountants and trust and company service providers can play in that context needs to be examined.[193]

Cryptocurrency Infrastructure

In order to obscure the provenance of tainted bitcoins, which is the dominant cryptocurrency so far, criminals employ the following techniques:

- Using virtual currency exchanges for either converting bitcoins into privacy focused coins (such as Monero or Dash) and back (a process known as 'chain-hopping'), or converting bitcoins into fiat currency.
- Using peer-to-peer (P2P) exchange platforms.
- Using mixers/tumblers.
- Using gambling websites.

For convenience, this paper refers to all these actors of the cryptocurrency economy (exchanges, P2P exchange platforms, mixers and gambling websites) as the cryptocurrency infrastructure.

Virtual Currency Exchanges

Virtual currency exchange services can be offered through either a website or a physical kiosk connected to the internet. Such kiosks are commonly known as bitcoin ATMs since most of them deal in bitcoin, although over a half are also reported to trade at least one other cryptocurrency.[194]

Virtual currency exchanges provide two principal types of services, namely the conversion of cryptocurrency into fiat currency or vice versa (via crypto-to-fiat exchanges) and the conversion of cryptocurrency into another cryptocurrency or vice versa, known as chain-hopping (via crypto-to-crypto exchanges).

Depending on the service provided, a virtual currency exchange will receive user A's bitcoins (or other cryptocurrency) from address X and pay a corresponding amount – minus transaction fees – to a designated address Y in another cryptocurrency, or to a bank account Z in one of the fiat currencies. If the exchange does not carry out CDD on user A, there is a risk that its services may be misused to launder the proceeds of crime. Given that the transfer to a bank account from a cryptocurrency exchange may trigger the bank's scrutiny, chain-hopping is particularly attractive to criminals due to the absence of any intermediary other than the crypto-to-crypto exchange.

193. For an analysis of intelligence gaps in relation to those professions' involvement in high-end money laundering, see Helena Wood et al., 'Known Unknowns: Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers', *RUSI Occasional Papers* (April 2018).
194. Melanie Kramer, 'The Future of Cryptocurrency ATMs Has Arrived', *Bitcoinist*, 5 August 2018.

A particular threat is posed by rogue exchanges that retain no customer records. It is common among cyber-criminals to use seven or eight accounts with various exchanges to launder criminal proceeds, especially those exchanges in jurisdictions with lax regulation.[195]

Box 5: Money Laundering via BTC-e

From July 2011 until July 2017, BTC-e was one of the largest bitcoin exchanges. It converted various cryptocurrencies, including bitcoin and Litecoin, into fiat currency, and vice versa. From 2011 to 2016, BTC-e received over 9.4 million bitcoins, worth $43 billion in November 2018 prices. According to the US Department of Justice, BTC-e 'lacked basic anti-money laundering controls' and was 'designed to help criminals launder their proceeds'. BTC-e was operated by a Seychelles-registered company, Canton Business Corporation. It also maintained a number of affiliated companies with bank accounts via which users could pay or withdraw fiat currency.

The US indictment issued in January 2017 alleges that over 530,000 bitcoins stolen from Mt. Gox were sent to three accounts controlled by Alexander Vinnik, the alleged administrator of BTC-e. These funds were allegedly exchanged into fiat currency and sent to bank accounts in Cyprus and Latvia. The indictment also claims that 'hundreds of thousands of dollars' in the proceeds of the CryptoWall ransomware were laundered via BTC-e. Vinnik was arrested in Greece at the request of the US. As of November 2018, France, Russia and the US are each seeking his extradition from Greece.

Sources: US vs BTC-e & Vinnik, 'Superseding Indictment', CR 16-00227 SI, United States District Court, Northern District of California, San Francisco Division, 17 January 2017; Josiah Wilmoth, 'Alleged Bitcoin Launderer Alexander Vinnik Questioned by French Investigators, Lawyer Says Charges are "Trumped Up"', CCN, *1 October 2018.*

P2P Exchange Platforms

P2P (decentralised) exchange platforms, such as LocalBitcoins, connect users to enable a direct exchange of cryptocurrency between them. Instead of purchasing from or selling to the exchange, the user of a P2P exchange who wishes to sell bitcoins is connected to a user willing to purchase the corresponding amount of bitcoins. Some P2P exchanges offer escrow services to facilitate transactions.[196] Alternatively, users can meet physically to exchange money for private keys, although geographic proximity is a prerequisite for that (hence the name LocalBitcoins). P2P exchanges have given rise to the phenomenon of rogue cryptocurrency traders, who are effectively in the business of facilitating money laundering.[197] Furthermore, new business

195. Clayton, 'Dave Jevans's Presentation'.
196. Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing', p. 41.
197. Author interview with a law enforcement officer, London, April 2018.

models of P2P exchanges may emerge in the future that will not rely on a single entity that administers the exchange and can carry out CDD controls and trace customers' transactions.[198]

Mixers/Tumblers

The abovementioned use of virtual currency exchanges pursues the purpose of breaking the chain of traceable bitcoin transactions. Enabling this is the sole purpose of bitcoin mixers, also known as 'tumblers'. To use a bitcoin mixer, user A sends bitcoins from an address X to a mixer and requests to transfer them to address Y (which is typically controlled by user A but can also be controlled by someone user A wants to pay). The mixer combines user A's bitcoins received from address X with bitcoins received from a multitude of other addresses and obscures the origin of each given bitcoin. Thereafter, the mixer sends to address Y the amount in bitcoins equal to user A's original input minus the mixer's fee. The process can be repeated with a variety of mixers if the user can afford the fees, which are typically around 3%.[199]

If the address used by the mixer to send bitcoins to user A is known to be associated with that mixer, the blockchain will show that address Y has received bitcoins from the mixer – as have thousands of other addresses – but will not enable linking addresses X and Y.[200] Mixers regularly change their output addresses to make it more difficult to establish that address Y has received funds from a mixer at all.[201]

The obscuring effect of mixer use can be overcome if there are ways to link addresses X and Y to user A, for instance if user A is careless enough to disclose their control over both these addresses on a public forum. Another way of penetrating the secrecy provided by mixers is to link the size or timing of incoming and outgoing transactions, but various techniques are employed by mixers to prevent this.[202] In short, tracing transactions obfuscated via mixers is possible but extremely challenging.[203]

According to Europol, there are some signs of a decline in the use of mixers. The two largest mixers, BitMixer and Grams Helix, shut down in 2017. Against that backdrop, Europol expects that the need for mixers will decline as privacy coins become ever-more widespread.[204]

198. The risk of 'automated, decentralised exchanges, which would require no KYC' is highlighted in Europol, *Internet Organised Crime Threat Assessment 2018*, p. 63.
199. Clayton, 'Dave Jevans's Presentation'.
200. Elliptic, 'Bitcoin Mixers: Assessing Risks in Bitcoin Transactions', 7 May 2018; Keith Collins, 'Watch This Extorted Money Get Lost in the Expanse of the Blockchain', *Quartz*, 17 July 2017.
201. Author telephone interview with a cryptocurrency expert, August 2018.
202. Arvind Narayanan, 'Mixing', video from the course by Princeton University, 'Bitcoin and Cryptocurrency Technologies', Coursera, <https://www.coursera.org/lecture/cryptocurrency/mixing-WAiaS>, accessed 16 October 2018.
203. Author interview with a law enforcement officer, London, March 2018.
204. Europol, *Internet Organised Crime Threat Assessment 2018*, p. 63.

Nonetheless, for the time being mixers remain in use. The risk they pose is exacerbated by the fact that mixers do not normally disclose their location and, when they do, the information is not always reliable.[205] As with crypto-to-crypto exchanges, there are therefore significant intelligence gaps as to the operation of mixers.[206] Clarifying the legal implications of mixing, as discussed in Chapter III, may give LEAs the means to pursue those mixers that are involved in illicit activities and provide the impetus towards addressing existing intelligence gaps.

Gambling Websites

There is evidence of cyber-criminals laundering tainted bitcoins through gambling websites that accept bitcoins.[207] The websites reportedly used to launder the proceeds of ransomware both accept and pay out bets in cryptocurrency (specifically bitcoin). The website of one such gambling outlet states: 'No personal information is needed to play our games'.[208] Although gambling services are covered by the EU's 4th Anti-Money Laundering Directive,[209] few cryptocurrency gambling websites, if any, disclose the jurisdiction of their incorporation.[210]

Off-Blockchain Transactions

To avoid detection risks associated with the transparency of the blockchain, a criminal may opt for a physical transfer of a private key. For instance, a criminal may hand over a hardware cryptocurrency wallet, a QR code containing the private key or a prepaid cryptocurrency card to another person in the same way as paying cash. Although such off-blockchain transactions happen offline, they can be arranged via P2P exchange platforms.

205. Author telephone interview with a cryptocurrency expert, August 2018.
206. *Ibid*.
207. Paquet-Clouston, Haslhofer and Dupont, 'Ransomware Payments in the Bitcoin Ecosystem', p. 6.
208. Bitzillions, <https://bitzillions.com/en/>, accessed 16 October 2018.
209. Council of the European Union, 'Article 1(3)(f) of Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing', *Official Journal of the European Union* (L141/73, 5 June 2015).
210. CipherTrace, 'Cryptocurrency Anti-Money Laundering Report', pp. 8–9.

Box 6: Prepaid Cryptocurrency Cards

Some LEAs view prepaid cryptocurrency cards as a priority area due to their potential money-laundering risks. Such cards were allegedly used by the Carbanak/Cobalt group. Cryptocurrency cards are issued by a financial institution (the card issuer) that participates in one of the payment-processing networks, such as Visa or MasterCard. The customer can use such a card to pay any merchant whose acquiring bank is a member of the respective payment-processing network. The financial institution issuing the card typically does so in partnership with a company (the card issuer's partner) that accepts the customer's funds in cryptocurrency and converts them into fiat currency that is used to fund the card. The card issuer's partner is likely to fall within the definition of a virtual currency exchange under 5AMLD and be responsible for CDD.

Sources: Author interview with a law enforcement officer, London, April 2018; Europol, 'Mastermind Behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain'; see also Europol, 'Carbanak/ Cobalt Infographic', <https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic>, accessed 16 October 2018; Business Wire, *'New York State Department of Financial Services Grants Virtual Currency License to BitPay', 16 July 2018.*

E-Commerce, E-Gambling and Online Gaming

In 2012, Moneyval noted money-laundering risks posed by 'online gaming and online trading platforms' but did not identify any specific cases where those risks had materialised.[211] Since then, there have been known instances of cyber-criminals laundering funds by purchasing and selling products within online multiplayer games.[212] Other methods of laundering funds online include paying for fake handyman job adverts[213] or fake trips.[214] While it has been argued that such methods make it 'possible to launder a large amount of money in small amounts through thousands of electronic transactions',[215] there is no confirmation of this happening. The perpetrators of a number of large-scale hacks against US financial institutions in 2014, including JP Morgan, operated an unlawful internet casino, but since this business was unlawful, they only engaged in it to generate illicit revenue rather than launder other criminal proceeds.[216]

211. Moneyval, 'Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction', March 2012, p. 57.
212. Rachel Kaser, 'Free-to-Play Games are a Breeding Ground for Money Laundering', *The Next Web*, 21 July 2018; Jean-Loup Richet, 'Laundering Money Online: A Review of Cybercriminals' Methods', UNODC, Cornell University Library, 1 June 2013, pp. 11–13.
213. Richet, 'Laundering Money Online', pp. 14–17.
214. Author telephone interview with a cyber-security expert, June 2018.
215. Richet, 'Laundering Money Online', p. 14.
216. US vs. Gery Shalon et al., 'Sealed Superseding Indictment', New York Southern District Court, Sl 15 Cr. 333 (LTS), 22 October 2015, paras. 17–19.

Use of Proceeds

Understanding the ultimate destination of cyber-criminal funds can help identify financial chokepoints, namely financial institutions or businesses such as real-estate agents, that may be unwittingly involved in the investment of the proceeds of cybercrime. However, opportunities for intervention are likely to depend on whether such businesses operate in jurisdictions with robust AML regimes, including whether the reports are followed up operationally.

At the moment, knowledge gaps exist in relation to how cyber-criminals use the proceeds of their offences, in particular regarding the prevalence of the following scenarios:

- Reinvestment in cybercrime.
- Reinvestment in other criminal activities.
- Investment in the legal economy or lifestyle purchases.

The only such assessment identified in the research for this paper has been conducted by Michael McGuire, who has reported based on 100 interviews and observations of Dark Web conversations that 15% of cyber-criminals spent funds on immediate needs (such as bills and food), 20% on disorganised or hedonistic spending, 15% on status items, 30% on assets such as property, and 20% reinvested the funds in criminal activity.[217] However, McGuire's report covers a much broader range of crime, including all illicit trade on the Dark Web and IP theft. Moreover, since it is likely that criminals spend funds towards several purposes rather than just one, further work in this area would add value to McGuire's research.

The sophistication and continuous refinement of some strains of malware suggests that criminals may be reinvesting their earnings into products or services necessary to improve their malware.[218] Yet there is no evidence that criminal groups in fact reinvest their funds in this rather than their time and effort. Similarly, in relation to reinvestment in other crimes, while some individuals found guilty of cybercrime also dealt drugs,[219] it is uncertain whether this is a widespread trend. There is also sporadic evidence of 'offline' organised criminal groups hiring cyber-criminals to work for them or investing funds into cyber-criminals' operations in return for a share of the profits.[220]

217. McGuire, 'Into the Web of Profit', pp. 100–15.
218. Nikita Slepogin, 'Dridex: A History of Evolution', Securelist, 25 May 2017; EAG, 'Typology Project: Cybercrime and Money Laundering', p. 32.
219. See the case of Grant West for example, *UK Breaking News,* 'Half a Million Pounds Worth of Bitcoin Seized from Prolific Hacker'; Rutger Leukfeldt and Jurjen Jansen, 'Cyber-Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands', *International Journal of Cyber Criminology* (Vol. 9, No. 2, 2015), pp. 17, 175 (referring to drug dealing and human trafficking).
220. Jonathan Lusthaus, 'Is the Mafia Taking Over Cybercrime?', paper presented to the Black Hat USA 2018 Conference, Mandalay Bay, 4–9 August 2018, <https://i.blackhat.com/us-18/Wed-August-8/us-18-Lusthaus-Is-The-Mafia-Taking-Over-Cybercrime-wp.pdf>, accessed 16 October 2018.

The potential for terrorist involvement in cybercrime is demonstrated by the case of three British terrorist sympathisers, Tariq Al-Daour, Waseem Mughal and Younes Tsouli, who by the time of their arrest in 2005 had earned up to £2 million by stealing credit card details and laundering the proceeds using e-gambling and e-Gold, a centralised virtual currency.[221] That example notwithstanding, there is no evidence of systematic terrorist involvement in cybercrime to raise funds.

In contrast to this, attacks that have been ascribed by some to the North Korean regime, such as the Bangladesh Bank heist, suggest that cyber-criminal activities may have funded nuclear proliferation. It has also been reported that North Korea may be benefiting from cryptojacking to mine Monero.[222]

Whatever the ultimate use of proceeds, financial investigations are critical in clarifying how the proceeds of cybercrime are used and what intervention opportunities are therefore available.

221. Clay Wilson, 'Cybercrime', in Franklin D Kramer, Stuart H Starr and Larry K Wentz (eds), *Cyberpower and National Security* (Washington, DC: National Defense University Press and Potomac Books, 2009), p. 432.
222. Joyce Lee, 'Cryptocurrency May be Getting Quietly Channelled to North Korea University – Report', *Reuters*, 8 January 2018.

III. Key Areas for Further Action

IN THE UK, regulated entities are obliged to conduct CDD and make suspicious activity reports (SARs) to the UK Financial Intelligence Unit (UKFIU). They therefore have a key role to play in supporting LEAs' efforts to target the proceeds of cybercrime. This chapter proposes measures to improve the detection of the proceeds of cybercrime and facilitate the sharing of relevant information between these sectors and LEAs.

On a practical level, both LEAs and regulated entities should consider what data points they can use to identify accounts involved in laundering the proceeds of cybercrime and how they can share this information with others. In terms of regulation and law-making, policymakers should consider responses to the challenges posed by some parts of the cryptocurrency infrastructure.

Financial Sector

Despite the technology-driven nature of cybercrime, those who engage in it often exploit the traditional financial sector. Key areas for the financial sector's response to the money-laundering threat posed by cybercrime relate to money-mule accounts and financial institutions' exposure to virtual currencies.

Money-Mule Accounts

Depending on the type of the money-mule account at hand, the challenges of detection will differ.

The ability of criminals to obtain money-mule accounts may to some extent be addressed by cyber security or anti-fraud policies.[223] For instance, protecting a customer's account against hacking falls within the scope of measures taken by financial institutions to ensure their own and their customers' cyber security. Such measures often include the analysis of cyber-security trends, including the monitoring of Dark Web markets.[224]

Similarly, financial institutions' efforts against the use of fraudulent ID documents do not depend on whether an account opened with a fake ID is going to be used for fraud, money muling or any other purpose. While policies and practices are in place to prevent the use of fake IDs, challenges are presented by the use of high-quality forgeries, foreign ID documents that front line staff in financial institutions have less knowledge of, and unlawfully obtained genuine documents.[225]

223. Author telephone interview with a bank, March 2018.
224. Author telephone interview with a money service business, July 2018.
225. Author interview with a law enforcement officer, London, May 2018.

The detection of money mules who use their accounts for cyber-criminals' benefit poses significant difficulties. It is extremely challenging to detect a money-mule account that was opened by a bona fide customer but then sold to a cyber-criminal, for instance because the owner no longer needed it.[226]

Three areas of work that have the potential to mitigate the challenges posed by money-mule accounts are: real-time tracing of money-mule transactions (based on following the money from the point of the transfer that is known to be fraudulent); the analysis of a broad range of data points to link money-mule accounts; and measures aimed at the disruption of money-mule recruitment.

Real-Time Transaction Tracing

The speed of transactions enabled by the UK's Faster Payments Scheme means that criminals can rapidly move money through a number of accounts with different UK banks.[227] Tracing the funds along the chain of money-mule accounts therefore requires cooperation between different banks, which takes time. By the time a bank has the grounds to freeze the funds, the money will often have been dissipated.[228] The challenge is particularly pronounced in relation to money-mule accounts that are several steps removed from the predicate offence.[229]

To address this issue, 12 financial institutions in the UK that take part in the Faster Payments Scheme are currently setting up a funds-in-flight monitoring system (the Mule Insights Tactical Solution) based on the proof of concept developed by Vocalink.[230] Operational since autumn 2018, the system will generate alerts on known fraudulent fund transfers – made from what is called a 'seed account' – and map the movement of those funds through accounts in other participating institutions.[231]

The system is expected to minimise the amount of time needed to identify the destination of criminal proceeds and freeze them. It will also enable a better understanding of how money-mule networks operate and where intervention opportunities exist. For instance, the pilot project suggests that there may exist 'a large, highly-connected central mule network in the UK (composed of c.25% of all suspect mule accounts)'.[232]

---

226. RUSI workshop on strengthening the anti-money laundering response to cyber-crime.
227. The challenge also arises in other countries with similar systems, such as Germany; see Check Point and Europol, 'Banking Trojans', p. 13.
228. Author interview with a law enforcement officer, London, March 2018; author interview with a bank, London, March 2018; author interview with a cyber-security expert, London, April 2018.
229. Author interview with an industry group, London, August 2018.
230. Faster Payments Scheme Limited, 'Faster Payments General Directions Compliance Report 2017', 2017, p. 35.
231. See Vocalink, 'The Rise of the Mule', 2017, p. 5.
232. *Ibid.*

Analysing a Broad Range of Data Points

Links between money-mule accounts operated by the same criminal(s) may be revealed by the analysis of data points connected to those accounts. Some of these data points are provided by the account holder during onboarding. Others relate to the individual's digital footprint that can be analysed when they log in to use online banking services.

Although details of use of cyber indicators cannot be disclosed in a public report, they have already been successfully used by LEAs to link money-mule accounts in non-cybercrime cases.[233] In addition, detecting changes in a customer's digital footprint may suggest that another person has started using the account.

This approach is particularly potent if combined with behavioural analysis of the customer's activity, such as their typical patterns of navigating the bank's website.[234] Furthermore, behavioural analytics can be used to identify accounts posing increased risk of involvement in money muling with a view to monitoring them.[235]

Some financial institutions also use behavioural analytics to prevent criminals from opening accounts in someone else's name, for instance by:

> analysing whether text may have been copied and pasted into an online application form (for example, by fraudsters attempting to make numerous applications); and observing the time taken to navigate websites or complete an application (for example, fraudsters may go through an application process very quickly, using information already generated from other fraudulent applications).[236]

Acknowledging a wide variety of possible applications of the customer's digital footprint, one bank states as follows:

> [W]hen opening an account, the financial institution (FI) can determine if the PII [personally identifiable information] provided matches the individual's digital identity. … Alternatively, the FI can determine if the digital identity of the prospective customer has been previously associated with different PII. … This can be very helpful in identifying and preventing potential money mule activity, as well as preventing new account fraud.[237]

---

233. Author interview with a law enforcement officer, London, March 2018.
234. Author interview with an industry group, London, August 2018.
235. Author telephone interview with a bank, April 2018.
236. FinTech Financial Crime Exchange, 'Disrupting Financial Crime: Best Practice in Customer Due Diligence Among Fintechs', May 2017, p. 7.
237. Standard Chartered, 'Understanding Digital Identities in the World of Cybercrime and Compliance', <https://www.sc.com/fightingfinancialcrime/av/SCB_Fighting_Financial_Crime_Deep_dive_Digital_Identities_December_2017.pdf>, accessed 16 October 2018.

Although cyber indicators have special relevance in the context of the proceeds of cybercrime, which is by definition committed online, such analysis can be done in relation to a broad range of data associated with a given customer.[238] An important caveat is that relevant information, such as IP or media access control (MAC) addresses, is relatively easy to obfuscate (in the case of IP addresses) or spoof (in the case of MAC addresses).[239]

The challenge is therefore to identify the types of data points and the methods of using them that are most feasible and produce the greatest impact while being proportionate in relation to possible privacy implications. To carry out this type of analysis, a degree of coordination is necessary between cyber security, AML/financial crime and fraud departments within financial institutions.[240] This is an area that some banks are increasingly addressing by revisiting their approaches to storing and sharing data within the company.[241] Another option is the creation of fusion cells that bring together the expertise and information from previously disparate units.[242]

Related initiatives concern improvements to the ability of banks to promptly freeze funds that enter accounts identified as posing a higher risk of being misused as money-mule accounts. For example, in case such an account is credited with an unusual amount, the relevant funds may be subject to a freeze pending an explanation from the account holder as to their origin.[243]

Information Sharing

In order to ensure the maximum yield from the aforementioned practices and since each institution is only likely to have some part of the data that it could usefully exploit, financial institutions should consider whether the sharing of relevant information would meet applicable data-protection standards, especially if it is necessary and proportionate to the objective.

Information sharing should pursue a defined purpose and be based on an analysis of the types of data that help achieve that purpose. One of the relevant considerations is ensuring the compatibility of data and agreeing on the format in which it is shared. Since banks employ different practices to analyse their customers' digital footprint, information sharing will only be effective if a given data point can feed into another bank's analysis.

Depending on the precise types of non-financial information that should be shared to enable better identification of money-mule accounts (in addition to current information-sharing efforts), the UK government and financial institutions will need to verify to what extent such data can be effectively shared via existing information-sharing arrangements. At the moment,

238. *Ibid.*
239. Author telephone interview with a law enforcement officer, July 2018.
240. Author telephone interview with a financial consultancy firm, March 2018; author telephone interview with a bank, March 2018; author interview with a bank, London, August 2018.
241. Author interview with a bank, London, August 2018.
242. The authors are grateful to one of the peer reviewers for their insight on this.
243. Author interview with a bank, London, August 2018.

several public–private partnerships in the UK enable the sharing of non-financial information, including cyber indicators:

- **Joint Money Laundering Intelligence Task Force (JMLIT):** The JMLIT was launched by a number of UK government agencies and financial institutions as a pilot project in early 2015 and was put on a permanent footing in May 2016. Its objective is to share financial and non-financial information, including IP addresses, among its members for both operational purposes and developing a common view of financial crime risks.[244] The JMLIT functions according to Section 7 of the Crime and Courts Act 2013, which authorises regulated entities to make disclosures to the NCA.[245]
- **Financial Crime Alerts Service (FCAS):** The FCAS is run by UK Finance to disseminate intelligence alerts based on the JMLIT's work to a broader audience.[246]
- **Cyber Security Information Sharing Partnership (CiSP):** The CiSP is run by the NCSC and is open to UK companies 'responsible for the administration of an electronic communications network in the UK',[247] which includes a number of financial institutions.[248] The CiSP is focused on cyber security and does not distribute information with a view to money-laundering prevention.[249]
- **Joint Fraud Task Force (JFTF):** The JFTF is chaired by the Home Office and brings together a range of LEAs and financial institutions.[250]
- **Virtual Task Force (VTF):** The VTF is run by the NCCU and brings together 26 retail banks. The VTF facilitates information sharing for operational purposes in relation to specific cases investigated by the NCCU.[251]
- **Cyber Defence Alliance (CDA):** The CDA brings together several banks to share information on cyber security and related financial crime threats. Its work covers issues such as money mules and the use of analytics for better money-laundering detection.

---

244. NCA, 'Joint Money Laundering Intelligence Taskforce (JMLIT)', <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit>, accessed 16 October 2018.
245. David Artingstall and Nick J Maxwell, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017), p. 13.
246. Matt Allen, 'Uniting to Tackle Financial Crime', *BBA*, 27 February 2015.
247. NCSC, 'Cyber Security Information Sharing Partnership (CiSP)', updated 20 March 2018, <https://www.ncsc.gov.uk/cisp>, accessed 16 October 2018.
248. Cabinet Office, 'Government Launches Information Sharing Partnership on Cyber Security', press release, 27 March 2013, <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security>, accessed 16 October 2018.
249. Author telephone interview with a financial consultancy firm, March 2018; Author telephone interview with a bank, April 2018.
250. City of London Police, 'Joint Fraud Taskforce Calls on the Public's Help to Catch Ten Wanted Fraudsters', 13 February 2017.
251. *Ibid.*

Box 7: US Experience of Information Sharing

The National Cyber-Forensics & Training Alliance (NCFTA), which was founded in 2002 and co-locates representatives from private industries and LEAs, has a dedicated Cyber Financial (CyFin) programme that looks at both cyber threats to the financial industry and financial crime threats resulting from cybercrime, similarly to the CDA but with a larger membership. The NCFTA has been a useful source of intelligence for both US and foreign law enforcement, including UK LEAs.

Sources: NCFTA, 'CyFin Program', <https://www.ncfta.net/cyfin-program/>, accessed 16 October 2018; RUSI workshop on strengthening the anti-money laundering response to cybercrime.

Including Cyber Indicators in SARs

While the current AML regime largely relies on regulated entities complying with their AML obligations and reporting suspicions of activity that involves criminal property, the reality is that often regulated entities cannot – and should not be expected to – identify the specific predicate offence concerned. For instance, a financial institution may report possible money-muling activity based on transactions that are inconsistent with the customer's profile but will frequently be unable to determine whether it relates to the proceeds of cybercrime or some other offence.

Yet from a law enforcement perspective, establishing the possible predicate offence is critical for disseminating the SAR to an appropriate investigative team. This difficulty is not limited to cybercrime and applies across the board. In particular, the challenges that arise from the high numbers of SARs received by the UKFIU are well-known and need not be rehearsed here.[252]

In this context, enabling the inclusion of cyber indicators in SARs in a standardised format will give more opportunities to LEAs to link and cluster suspicious activities.[253] This may help identify malicious actors and the type of criminality concerned. Some financial institutions already file cyber indicators in SARs in the UK, but only on a case-by-case basis if they are seen as particularly relevant.[254] Including a standardised format or field for this information would both facilitate its analysis and encourage reporting entities to submit it whenever relevant.

252. See, for example, Law Commission, 'Anti-Money Laundering: The SARS Regime', Consultation Paper No. 236, July 2018, paras. 4.1–4.17.
253. Author telephone interview with a data analytics company, July 2018.
254. Author interview with a money service business, London, July 2018.

Box 8: US and Australian Experience of Including Cyber Indicators in SARs

In 2016, the US Financial Crimes Enforcement Network (FinCEN) issued guidance requiring SARs to include available cyber-related information, which encompasses 'technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs)', as well as 'data regarding the digital footprint of individuals and their behavior'. FinCEN's requirement applies to any SARs, not only those related to cyber security breaches. The issuance of the advisory reflected the feeling among US LEAs that even although such cyber indicators as IP addresses can be easily spoofed, the value they have for some investigations justified their collection and analysis. Australia also requires the reporting of IP addresses, unique device identifiers (defined as '[MAC] addresses, International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI) numbers, and secure element ID (SEID) numbers') and social media identities, for transactions involving virtual currency.

Sources: FinCEN Advisory FIN-2016-A005, 'Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime', October 2016. A more detailed, but non-exhaustive list of cyber-related information is available at Financial Crimes Enforcement Network, 'Frequently Asked Questions Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information Through Suspicious Activity Reports', 25 October 2016, <https://www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-events-cyber-enabled-crime-and-cyber>, accessed 23 November 2018; 'Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (Australia)', No. 1, Sections 18.4(2), 18.2(21A), 19.1(8) and 19.6(3); RUSI workshop on strengthening the anti-money laundering response to cybercrime.

Disruption of Money-Mule Recruitment

Efforts aimed at rendering money-mule recruitment more costly and difficult have the potential to disrupt the money-laundering infrastructure that services cyber-criminals. There are at least three areas where such efforts can be focused: awareness-raising among potential money mules; liaising with social media platforms to take down money-mule recruitment advertisements; and sting operations by law enforcement officers that pose as providers of money-mule networks or set up bogus money-mule accounts.

Awareness-raising initiatives already form a key part of efforts against money muling,[255] but need to be reassessed and retargeted on an ongoing basis to directly address those demographics most at risk. For instance, according to some interviewees, a recent trend in the UK is the increased use of secondary school students.[256] Awareness-raising can focus both on legal risks to money mules and on the social consequences of their actions, such as harm to the victims of cybercrime.

255. See, for example, Financial Fraud Action and Cifas, 'Don't Be Fooled', <https://www.moneymules.co.uk/>, accessed 23 November 2018.
256. Author interview with a bank, London, August 2018.

Advertisements posted on social media are reportedly a prominent means of money-mule recruitment, which opens up opportunities for disruption by means of taking down such content.[257]

Setting up bogus money-mule accounts by law enforcement can enable recouping stolen funds transferred through such accounts and/or gaining intelligence on cyber-criminal networks. Furthermore, the risk of ostensible money mules or money herders being law enforcement officers can erode the trust that cyber-criminals have in online money-mule recruitment and therefore make it more difficult. Together with the quality of the services provided, the true identity of the counterpart is one of the two major sources of uncertainty in cyber-criminal transactions.[258]

Exposure to Cryptocurrency

Virtual currency exchanges are not isolated from the traditional financial sector. Crypto-to-fiat exchanges and other cryptocurrency businesses, such as mining pools,[259] require bank accounts to make and receive payments from their customers. Similarly, banks serve customers that receive payments from cryptocurrency exchanges. Whether such transactions in and of themselves trigger AML alerts differs among banks.[260]

Box 9: Suspicious Activity Report in Relation to a Bitcoin-Financed Purchase

Tomáš Jiříkovský, the administrator of the Dark Web market Sheep Marketplace, was sentenced to nine years in prison in the Czech Republic after he stole the equivalent of $731,600 in bitcoin from the market's users. He invested $345,000 derived from the sale of bitcoins into purchasing a house, which was subsequently seized by law enforcement. According to press reports, the Czech investigation was triggered by a suspicious transaction report received from the bank where his partner had her account in relation to the transfer of $35,000 from a bitcoin exchange to her.

Sources: BayPay Forum, *'Czech Police Seize $345,000 Property Linked to Bitcoin Hack', 1 April 2015;* Deep Dot Web, *'Sheep Marketplace Owner Indicted and Faces Years in Prison', 21 April 2017.*

It is also possible that some financial institutions are not aware that a given customer is acting as a virtual currency exchange, for instance whether 'any customers are acting as unlicensed

257. Author interview with a bank, London, August 2018; author interview with a bank, London, April 2018.
258. Michael Yip, Craig Webber and Nigel Shadbolt, 'Trust Among Cybercriminals? Carding Forums, Uncertainty and Implications for Policing', *Policing and Society* (Vol. 23, No. 4, 2013), pp. 516, 522.
259. Arrangements for pooling computing power together to mine cryptocurrency and distribute profits therefrom.
260. RUSI workshop on strengthening the anti-money laundering response to cybercrime.

crypto brokers on sites such as LocalBitcoins.com'.[261] It is therefore important for institutions to assess their potential exposure through independent verifications (for example by screening customer data in light of available information about known exchanges).

In the absence of clear regulation of exchanges, the awareness of potential risks has led banks to adopt a cautious approach and has made it extremely difficult for cryptocurrency-based businesses in the UK to open bank accounts.[262] Over time, this situation can hamper innovation and drive cryptocurrency businesses to jurisdictions with lax AML controls.

The regulation of exchanges under 5AMLD, which is discussed in the following section, may therefore have the welcome consequences of clarifying AML standards applicable to cryptocurrency businesses and facilitating the banks' risk assessments. If based on a risk-based approach rather than a blanket rejection of cryptocurrency businesses, the banks' caution may provide an additional stimulus for crypto-to-fiat exchanges to establish robust AML controls, as many of the legitimate ones have already done. The fact that crypto-to-crypto exchanges, including some P2P exchanges, do not necessarily interact with banks and therefore do not have this stimulus for AML compliance, reinforces the argument that they should also be subject to AML regulations.

Cryptocurrency Infrastructure

Alongside the financial sector, cryptocurrency infrastructure is vulnerable to misuse by those who seek to launder the proceeds of cybercrime. This is the consequence of cryptocurrency being the preferred payment medium for transactions among cyber-criminals, and of the growth of crimes such as ransomware, theft of cryptocurrency and cryptojacking. While the value of analysing and sharing cyber indicators is also evident in the context of cryptocurrency businesses, the priority is devising appropriate legal and regulatory responses to risks posed by crypto-to-crypto exchanges, mixers and privacy coins, which this section considers.

261. FINTRAIL, 'Cryptocurrencies: Getting Serious About Financial Crime Risk Management', August 2018, p. 10.
262. Martin Arnold, 'Cryptocurrency Companies Forced to Bank Outside UK', *Financial Times*, 23 October 2017.

Box 10: Reporting of Suspicious Activity Involving Cryptocurrency

The guidance issued by the Australian Transaction Reports and Analysis Centre (AUSTRAC) provides several examples of scenarios that may warrant the submission of a suspicious matter report by a virtual currency exchange, such as:

- The customer's IP address disclosing information about their location that is inconsistent with the documents provided during onboarding.
- Transactions with an 'illicit marketplace, tumbler or illegal off-shore wagering website'.
- Large purchases of virtual currency suggestive of operating an unlicensed virtual currency exchange.

Source: AUSTRAC, 'A Guide to Preparing and Implementing an AML/CTF Program for Your Digital Currency Exchange Service Business', April 2018, pp. 18–20.

Regulation of Virtual Currency Exchanges

Rationale for Regulation

Although Bitcoin was conceived as a decentralised currency, many users rely on intermediary businesses to carry out transactions in bitcoin and other cryptocurrencies.[263] Virtual currency exchanges and wallet providers that hold cryptocurrency on behalf of their customers represent chokepoints that are both amenable to regulation and have a role in facilitating cryptocurrency transactions, some of which may be related to criminal proceeds. The significance of this for AML efforts is evident from the fact that as early as 2014 a UK police investigation was triggered by a SAR submitted by a virtual currency exchange based in continental Europe, despite the absence of a legal obligation on the part of the exchange to do so.[264]

In order to link incoming transfers to a virtual currency exchange with outgoing transfers, CDD and customer data retention is vital. Furthermore, recent research shows that many cryptocurrency exchanges settle transactions between their customers on their internal ledgers so that these transactions are never reflected on the blockchain.[265] The absence of traceable transactions on the blockchain in such circumstances highlights the importance of CDD and data retention.

The EU recognised the need for regulation in the domain of cryptocurrency. 5AMLD, which came into force on 9 July 2018 and must be implemented by EU member states by 10 January 2020, has extended AML obligations to 'providers engaged in exchange services between virtual currencies and fiat currencies' (crypto-to-fiat exchanges) and 'custodian wallet providers', or 'entit[ies] that provides services to safeguard private cryptographic keys on behalf of [their]

263. Carlisle, 'Virtual Currencies and Financial Crime: Challenges and Opportunities', pp. 13–14.
264. Author telephone interview with a law enforcement officer, March 2018.
265. Ross Anderson et al., 'Bitcoin Redux', 28 March 2018, pp. 13–19.

customers, to hold, store and transfer virtual currencies'.[266] Since criminals are likely to resort to exchanges located elsewhere, the UK government has undertaken to 'consult on whether to require firms based outside the UK to comply with [UK AML] regulations when providing services to UK consumers'.[267]

Although AML regulation extends to crypto-to-fiat exchange services irrespective of whether they are provided via a website or an ATM, there is evidence that some market participants are not certain about that and would welcome an explicit clarification to that effect from the regulators.[268] The report of the UK government's Cryptoassets Taskforce states that, when implementing 5AMLD, the government intends to consult on the regulation of 'cryptoasset ATMs, which could be used anonymously to purchase cryptoassets'.[269]

While obligations extended to virtual currency exchanges under 5AMLD are the same as those that apply to other businesses, the technical features of virtual currencies offer opportunities (such as blockchain tracing tools) that may not exist in other parts of the financial sector. In order to ensure the most effective mitigation of financial crime risks, supervisors should publicise and recognise innovative approaches designed to harness those opportunities.

P2P Exchange Platforms

Whether regulators will deem P2P exchange platforms to fall within the scope of 5AMLD remains to be seen. It has been argued that they are very difficult to regulate because 'they are not run by an entity or company that oversees and processes all trades, but they are operated exclusively by software (i.e. there is no central point of authority)'.[270] However, some of the largest P2P exchange platforms are run by individuals or companies who receive fees for at least

266. Council of the European Union, 'Articles 1 and 2(c) of the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU', *Official Journal of the European Union* (L156/43, 19 June 2018).
267. HM Treasury, Financial Conduct Authority and Bank of England, 'Cryptoasset Taskforce: Final Report', October 2018, p. 42.
268. Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing', p. 51.
269. HM Treasury, Financial Conduct Authority and Bank of England, 'Cryptoasset Taskforce: Final Report', p. 42.
270. Robby Houben and Alexander Snyers, 'Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion', study requested by the TAX3 committee, July 2018, p. 27.

some of the services offered.[271] These exchanges also already require ID verification either for all users,[272] or for those with 'significant' trading volumes.[273]

According to one interviewee, the decentralised nature of such exchanges means they do not hold the same amount of customer data as centralised exchanges.[274] Possible developments in exchanges' business model, such as the lack of a single entity running the exchange, may further affect their ability to identify customers and monitor transactions, which is why this sector requires ongoing attention. However, regulation should not be dismissed without further research into its feasibility and benefits.

Crypto-to-Crypto Exchanges

5AMLD does not cover crypto-to-crypto exchanges, which enable chain-hopping as a means of breaking the traceability of blockchain transactions. The Directive therefore does not address a crucial category of enablers of transaction anonymity.[275] Internationally, approaches to the issue differ. For instance, while the US extends its AML regime to both crypto-to-fiat and crypto-to-crypto exchanges, Australia only imposes AML obligations on crypto-to-fiat exchanges.[276] Given that chain-hopping can render it impossible to trace the provenance of a person's funds, there is no principled reason for leaving crypto-to-crypto exchanges outside the scope of AML regulations.[277]

In some cases, the practical impact of regulation may be limited depending on the location of a given exchange. However, the absence of regulation leaves LEAs and regulators with few tools to even try to address rogue crypto-to-crypto exchanges.[278] Bringing such exchanges within the scope of AML rules would fill that gap and enable the UK to raise the issue of regulating crypto-to-crypto exchanges with other jurisdictions. Developing a better intelligence picture of the activities and location of rogue virtual currency exchanges, including crypto-to-crypto exchanges, is essential to focus such international engagement efforts.

---

271. See LocalBitcoins.com, 'About LocalBitcoins.com', <https://localbitcoins.com/about>, accessed 16 October 2018; Steve Walters, 'xCoins for Beginners: Complete Review', *Unblock*, 17 May 2018, <https://unblock.net/xcoins-for-beginners-complete-review>, accessed 16 October 2018. It is worth noting that LocalBitcoins details the information it collects regarding the activities of its customers for the purposes of, among other things, money-laundering prevention, see LocalBitcoins.com, 'Privacy Policy', 9 May 2018, <https://localbitcoins.com/privacy_policy/>, accessed 16 October 2018.
272. Xcoins, 'How Does It Work?', <https://xcoins.io/how-it-works>, accessed 16 October 2018.
273. *Coinfox*, 'LocalBitcoins Starts Requiring ID Verification', 17 April 2018.
274. Author telephone interview with a law enforcement officer, April 2018.
275. Keatinge, Carlisle and Keen, 'Virtual Currencies and Terrorist Financing', p. 64.
276. *Ibid.*, pp. 47–49.
277. *Ibid*., p. 64.
278. Author telephone interview with a cryptocurrency expert, August 2018.

Clarifying the Implications of Mixers

Another challenge is presented by mixers, that is web services designed to ensure anonymous transactions and that are antithetical to CDD or reporting. Their proponents view mixers as a value-neutral privacy tool.[279] It is remarkable against this background that the once-largest mixer, BitMixer, shut down in July 2017, with its final statement extolling the transparency of Bitcoin's blockchain and predicting that '[v]ery soon this kind of activity [mixing] will be considered as illegal in most … countries'.[280]

Even though only around 16% of all bitcoins passing through mixers derive from provably illicit sources,[281] given the concerted international effort against anonymous financial transactions,[282] the acceptance of mixers is an anomaly. Given that mixers exist to ensure anonymous transactions, efforts to ensure that the use of cryptocurrency is in line with AML objectives need to address mixers.

There are several possible approaches to doing so. In the US, FinCEN Director Kenneth A Blanco suggested in August 2018 that mixers fell within the definition of MSBs under US AML regulations and were therefore subject to AML obligations under the Bank Secrecy Act 1970.[283] In practice, this means that mixers falling within US jurisdiction need to adjust their business model accordingly or face the risk of enforcement action, the latter being more likely given that anonymity is the mixers' raison d'être. Another way of addressing the use of mixers could be exploring the feasibility of attaching legal liability to the provision of mixing services. Finally, governments could abstain from seeking to regulate or prohibit mixers and instead clarify how virtual currency exchanges should treat transactions in coins that are known to have gone through mixers.

279. Narayanan, 'Mixing'.
280. Catalin Cimpanu, 'Internet's Largest Bitcoin Mixer Shuts Down Realizing Bitcoin is Not Anonymous', *Bleeping Computer,* 30 July 2017.
281. Yaya J Fanusie and Tom Robinson, 'Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services', FDD's Center on Sanctions and Illicit Finance and Elliptic, 12 January 2018, p. 8.
282. Such as the prohibition of anonymous accounts in financial institutions by the FATF Recommendations and the regulation of 'bearer shares'. See FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations', February 2012, revised October 2016, Interpretive Note to Recommendation 24, p. 86.
283. Kenneth A Blanco, 'Prepared Remarks of FinCEN Director Kenneth A Blanco', speech given at the 2018 Chicago-Kent Block (Legal) Tech Conference, 9 August 2018, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>, accessed 16 October 2018.

Anticipating Novel Cryptocurrency Business Models

The rapid changes to the cryptocurrency infrastructure highlight the need for a regulatory framework that is sufficiently flexible to accommodate new cryptocurrency business models. In line with 5AMLD, the UK will add virtual currency exchanges and custodian wallet providers to the list of businesses subject to AML regulations. This represents an opportune moment for deciding on a regulatory framework that is flexible enough to cover potential new cryptocurrency-related business models that pose money-laundering risks, as and when they emerge. Indeed, the UK government has announced its intention to go beyond 5AMLD and consult on the inclusion of crypto-to-crypto exchanges, P2P exchanges, bitcoin ATMs and non-custodian wallet providers in the UK's AML regime.[284]

The FATF Recommendations reinforce the need for a flexible approach that can be applied to emerging business models. In October 2018, the FATF introduced the definitions of 'virtual assets' and 'virtual asset service providers' so that such service providers become subject to AML regulation, provided they are not yet covered.[285] 'Virtual asset service providers' are defined in an expansive manner and include, among other things, businesses that are engaged in 'exchange between one or more forms of virtual assets' or 'transfer' of such assets. The FATF's reference to virtual assets forms part of Recommendation 15,[286] which also contains a broad requirement to identify, assess, manage and mitigate money-laundering risks posed by new products and new business practices. In view of the need for agile and responsive regulation, it is now up to states to choose the optimum means of ensuring that their AML frameworks address cryptocurrency-related risks, either by introducing new definitions of regulated businesses or by revising and expanding existing ones.[287]

Clarifying the Implications of Privacy Coins

Tackling the challenges posed by mixers would raise the broader question of dealing with privacy-focused coins, which are designed in such a way as to make tracing impossible or exceedingly difficult, and therefore effectively contain an 'inbuilt' mixing mechanism. Privacy features in no way detract from legitimate uses of privacy coins; neither do they suggest any impropriety on the part of those who create such cryptocurrencies. However, in order for privacy coins to gain widespread acceptance as means of payment, their potential money-laundering risks need to be addressed.

---

284. HM Treasury, Financial Conduct Authority and Bank of England, 'Cryptoasset Taskforce: Final Report', p. 42.
285. FATF, 'International Standards on Combating Money Laundering', Recommendation 15, p. 15, and Glossary, pp. 124–26, both updated October 2018.
286. *Ibid.,* p. 15.
287. For instance, the US FinCEN stated as early as 2013 that virtual currency exchanges, including those that conduct crypto-to-crypto transactions, fall within the scope of MSBs as defined under US AML regulations. See FinCEN, 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', FIN-2013-G001, 18 March 2013, p. 5.

In a submission to the House of Representatives' Financial Services Committee, a representative of the US Secret Service called for considering legislative or regulatory action to address the risks posed by privacy coins.[288] However, to date the US government has not chosen to enact specific regulation of privacy coins. In May 2018, the New York State Department of Financial Services authorised a virtual currency exchange to trade in the privacy coin ZCash.[289] The announcement on the ZCash official blog highlights that the exchange in question, Gemini, 'must adhere to all anti-money laundering (AML) laws [and] know your customer (KYC) requirements'.[290]

The existing US approach therefore relies on requiring virtual currency exchanges to establish the source of funds involved in privacy coin transactions as part of transaction monitoring. Whether transactions in any given coin are permissible will then depend on the extent to which exchanges can establish and document the source of funds.[291] In effect, this approach dissuades exchanges from transacting in coins that possess certain privacy features unless these can be mitigated through practical measures. As relevant experience is developed in the area, regulators have a potential role to play in setting out guidance on what such practical measures could look like.

In contrast, some commentators propose going further and 'prohibit[ing] exchanges from buying and selling cryptocurrencies that are explicitly designed to evade money-laundering and terrorist financing controls'.[292] A 2018 report commissioned by the European Parliament argues that doing so is 'worthwhile to consider'.[293] While potentially feasible, this approach requires developing consistent criteria for determining which cryptocurrencies should be off limits by virtue of being specifically designed for money laundering.[294]

In between the extremes is the stance taken by the Japanese Financial Services Agency, which has been discouraging exchanges operating in Japan from dealing in certain privacy coins.[295] Policymakers should take account of the experience of states at the forefront of regulation such

288. Novy, remarks at the hearing entitled 'Illicit Use of Virtual Currency and the Law Enforcement Response', p. 8.
289. New York Department of Financial Services, 'DFS Authorizes Gemini Trust Company to Provide Additional Virtual Currency Products and Services', press release, 14 May 2018, <https://www.dfs.ny.gov/about/press/pr1805141.htm>, accessed 16 October 2018.
290. Zooko Wilcox and Josh Swihart, 'Gemini Announces Support for Zcash', Zcash Company Blog, 14 May 2018.
291. Author telephone interview with a cryptocurrency expert, August 2018.
292. Anderson et al., 'Bitcoin Redux', p. 28.
293. Houben and Snyers, 'Cryptocurrencies and Blockchain', p. 83.
294. Author telephone interview with a cryptocurrency expert, August 2018.
295. Jake Adelstein, 'Japan's Financial Regulator is Pushing Crypto Exchanges to Drop "Altcoins" Favored by Criminals', *Forbes*, 30 April 2018. It has also been reported that the FSA has subsequently banned several privacy coins, see Andreas Townsend, 'Japan's Coincheck Removes Monero and Other Privacy Coins on FSA Ban', *Oracle Times*, 28 May 2018.

as Japan and the US when considering how best to address money-laundering risks posed by privacy coins, preferably on a coin-by-coin basis.

Conclusions and Recommendations

FINANCIALLY MOTIVATED CYBERCRIME involves a wide variety of monetisation and money-laundering techniques, which reflect the perpetrators' ingenuity. With security threats posed by cybercrime long recognised, efforts are increasingly underway to address the related financial crime risks. Doing so is not only a matter of implementing the AML regime, but also a valuable method of disrupting cyber-criminal operations and providing leads to LEAs.

The challenges posed by cybercrime to existing AML efforts largely fall within two broad themes. First, despite the novelty of cybercrime, its perpetrators frequently rely on the time-tested practice of using money-mule accounts. These are obtained in several ways, including by hiring unwitting members of the public. Company accounts are also used for laundering larger amounts. Second, cyber-criminal proceeds are often laundered via the cryptocurrency infrastructure. This reflects the growth in crime that generates proceeds in cryptocurrencies, as well as illicit trade on Dark Web marketplaces.

Responses to these challenges should take place at three levels. First, it is necessary to build a better knowledge base in relation to the modus operandi of enablers that wittingly or unwittingly facilitate cyber-criminal activities. Second, on an operational level, both LEAs and regulated entities should consider what data points they can use to identify accounts involved in laundering the proceeds of cybercrime and how they can share this information with others. This should complement ongoing efforts to trace and map money-mule transactions. Third, cryptocurrency-related risks require a targeted response, including guidance to the regulated sector to address the challenge of mixers and privacy coins.

Recommendations

Building the Knowledge Base

Recommendation 1

LEAs, policymakers and regulated entities should develop a better knowledge base in relation to the modus operandi of money-laundering enablers that facilitate cyber-criminal activities. In particular, they should aim to fill the following intelligence gaps:

- The modus operandi, identity and location of professional money launderers that incorporate companies for cyber-criminals and provide advice on money laundering.

- The modus operandi, identity and location of individuals who specialise in facilitating anonymous cryptocurrency transactions (for example, via mixers) and thereby wittingly or unwittingly facilitate the laundering of cyber-criminal proceeds.

Rationale

In recent years, considerable work has been done on money-mule accounts and mule herders, in particular through initiatives such as Europol's European Money Mule Action and associated activities by UK LEAs. However, there has been less focus on the activities of other professional money launderers, including those that provide sophisticated cybercrime groups with corporate accounts necessary to launder the proceeds of high-value, targeted attacks.

At the same time, the emergence of the cryptocurrency infrastructure has given rise to new types of businesses whose services can be used for money-laundering purposes. Some of these pose particular risks due to being unregulated to date (crypto-to-crypto exchanges), others by virtue of their business model (mixers). Developing a better intelligence picture as to the identity and location of individuals or groups that run such businesses will:

- Help regulators assess the likely impact of domestic regulation and set priorities for international engagement.
- Help LEAs identify intervention opportunities.
- Help regulated entities develop typologies and red flags that reflect money-laundering risks related to cybercrime.

Recommendation 2

LEAs, policymakers and regulated entities should develop a better knowledge base in relation to the end use of the proceeds of cybercrime.

Rationale

The ongoing work on money mules has contributed to a better understanding of the intermediary accounts that cyber-criminals use to receive funds from the victim's account and pass them on. Little is known on the ultimate destination of funds. Depending on whether these are deposited in a bank account or used to finance lifestyle purchases, regulated entities such as financial institutions, real-estate agents or high-value dealers may come into contact with the proceeds of cybercrime. Understanding the extent to which this is happening and the jurisdictions where those entities are located can help target law enforcement and regulatory efforts or prioritise international engagement with certain countries.

Detecting Money-Mule Accounts

Recommendation 3

When developing analytics techniques to detect money-laundering activities and identify the actors behind them, LEAs and regulated entities should rely on both financial crime and cyber-security expertise to determine what data points and analysis techniques are most relevant in the context of cybercrime.

If sharing particular types of data among financial institutions proves necessary to ensure effective detection of money-mule accounts and is proportionate to implications for privacy, UK government stakeholders (especially the Home Office and the NCA) and the regulated sector should verify to what extent this data can be effectively shared via existing information-sharing arrangements.

In order to ensure that regulated entities share relevant non-financial information both among themselves and with LEAs, the UKFIU should consider enabling the inclusion in SARs, in a standardised format, of cyber indicators including but not limited to IP addresses and device IDs.

Rationale

Since cybercrime by definition is committed online, its digital footprint may involve a range of data points beyond those that are traditionally analysed by LEAs and financial institutions for money-laundering prevention. Using these data points and analysing them together with other available information is a promising approach to detecting the proceeds of cybercrime, and potentially those of other offences with a digital footprint. This analysis should be done not only by financial institutions, but also by LEAs and other businesses that are regulated for AML purposes or will be regulated shortly, such as virtual currency exchanges.

Recommendation 4

Whenever feasible, regulated entities – including, where relevant, regulated cryptocurrency businesses – should aim to share their experience of innovation with respect to detecting the proceeds of cybercrime or other predicate offences, in particular in relation to:

- Real-time information sharing to trace the proceeds from a known fraudulent transfer down the chain of money-mule accounts.
- Analysing a wide range of data points, including cyber indicators such as IP addresses and device IDs, to link related accounts.

Rationale

Although the research for this paper confirms that some of the nascent practices may be too sensitive to be broadcast to a wide audience, regulated entities should strive to inform each

other of successful innovations as much as possible, with a view to benefiting from each other's work. The areas listed above are examples of such initiatives. In the end, sharing best practices may contribute to not only better targeting of the finances of cybercrime, but also those of other crimes with a digital footprint.

Addressing Cryptocurrency-Related Risks

Recommendation 5

When extending AML regulations to virtual currency exchanges and custodian wallets (whether through the adoption of new rules or a clarification of existing rules), the Home Office and HM Treasury should ensure that such regulations also capture other cryptocurrency-related business models posing money-laundering risks.

Rationale

While the implementation of 5AMLD will go a certain way towards addressing money-laundering risks related to virtual currencies, leaving the risks posed by other business models unaddressed could undermine the effectiveness of the regulatory response. Relevant business models that are not covered by 5AMLD include crypto-to-crypto exchanges, peer-to-peer (decentralised) exchanges, and mixers. In light of this, the UK government has announced its intention to 'go beyond the 5MLD requirements' and consult on the inclusion of crypto-to-crypto exchanges, decentralised exchanges, bitcoin ATMs, and non-custodian wallet providers in the UK's AML regime.[296] It is important for regulations to be sufficiently flexible to also address other cryptocurrency models that already pose or will in the future pose significant money-laundering risks. For instance, the consultation should also cover mixers. Although businesses such as mixers are relatively unlikely to comply with AML regulation given that it runs against the basis of their business model, subjecting them to AML obligations would create a legal foundation for taking enforcement measures.

The need to manage and mitigate money-laundering risks arising from cryptocurrency businesses is now acknowledged in the revised FATF Recommendations, which are sufficiently broad to cover all the aforementioned types of cryptocurrency businesses.

Recommendation 6

The relevant supervisor (once designated) should provide practical guidance to regulated virtual currency exchanges on dealing with higher-risk counterparties, such as mixers or unregulated exchanges, and transacting in higher-risk cryptocurrencies, such as privacy coins.

296. HM Treasury, Financial Conduct Authority and Bank of England, 'Cryptoasset Taskforce: Final Report', p. 42.

Rationale

Guidance will be critical to the effectiveness of any future regulations and to the ability of exchanges to navigate money-laundering risks. Similar to guidance issued for other sectors, guidance should raise awareness on how exchange services may be misused for money-laundering purposes. It would also help exchanges prioritise their mitigation measures.

About the Authors

Anton Moiseienko is a Research Analyst at RUSI's Centre for Financial Crime and Security Studies. His current research covers a range of financial crime issues, including corruption and financial integrity in developing countries, global responses to terrorist financing, and the intersection between cybercrime and money laundering. Prior to joining RUSI, Anton completed his PhD in law at Queen Mary University of London.

Olivier Kraft is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies. His research interests include the opportunities of new technologies for anti-money laundering (AML) efforts, and the synergies between AML and cyber-security measures. Prior to joining RUSI in 2017, Olivier worked with the Financial Action Task Force (FATF), the global standard-setter in the areas of AML/counterterrorist finance (CTF), where he focused on evaluating the effectiveness of countries' AML/CTF efforts. From 2011 to 2015, Olivier advised the World Bank Group Sanctions Board on allegations of fraud and corruption in development projects co-financed by the World Bank Group.