Royal United Services Institute
for Defence and Security Studies

BRIEFING PAPER

Rethinking the UK Response to Cyber Fraud

Key Policy Challenges

Sneha Dawda, Ardi Janjeva and Anton Moiseienko

EXECUTIVE SUMMARY

- This paper outlines the challenges faced in responding to the threat from cyber-enabled fraud in the UK, and provides an overview of the challenges in combating cyber fraud over the next decade and beyond. This forms part of a wider project which will include a research paper due for publication in early 2021. This next phase will provide actionable policy recommendations based on in-depth primary research with law enforcement agencies, financial institutions and other key stakeholders.
- Recent years have seen a worrying increase in reported fraud offences. At the same time, the ongoing public health crisis has amplified the need for the private sector to maintain a vigilant cyber security posture against the three main phases of the cyber fraud lifecycle: the cyber attack phase; data exploitation; and the cash-out phase. These comprise the cybercrime business model.
- There are three main barriers that have prevented law enforcement and the financial sector from reducing the impact of cyber fraud in the UK over the past decade: reporting; investigation; and enforcement barriers.
- Existing UK structures to tackle cyber fraud have not yet delivered the law enforcement outcomes that are needed. A fundamental reassessment is required of the law enforcement response to cyber fraud at the national and local level, as well as a clearer articulation of the roles and responsibilities across the financial sector.

INTRODUCTION

Cyber-enabled fraud (referred to throughout this paper as 'cyber fraud') is a crime with high impact on citizens and society as a whole.[1] Future policy must take these individual and societal harms into account and assign clear roles and responsibilities to tackle the threat. This paper provides an overview of the challenges in combating cyber fraud over the next decade and beyond. While the paper outlines numerous challenges, the cyber fraud policy area remains relatively new and attempts at public–private sector co-production of responses and solutions do exist.[2] A RUSI research paper to be published in early 2021 will provide policy recommendations in overcoming barriers and suggesting improvements to the current model.

1. According to the Scottish Crime and Justice Survey, one in five people will be a victim of cyber fraud or computer misuse crimes. See *BBC News*, 'One-in-Five Experiences Cyber Fraud Each Year', 16 June 2020. For the purposes of this paper, 'cyber fraud' is the use of the internet to enable or commit the theft of property (including money) by dishonest means. As per Section 7 of the Fraud Act (2006), any persons making or supplying articles – data in the case of cyber fraud – are also liable.
2. See, for example, N8 Policing Research Partnership, 'Annual Report', <https://n8prp.org.uk/>, accessed 5 June 2020.

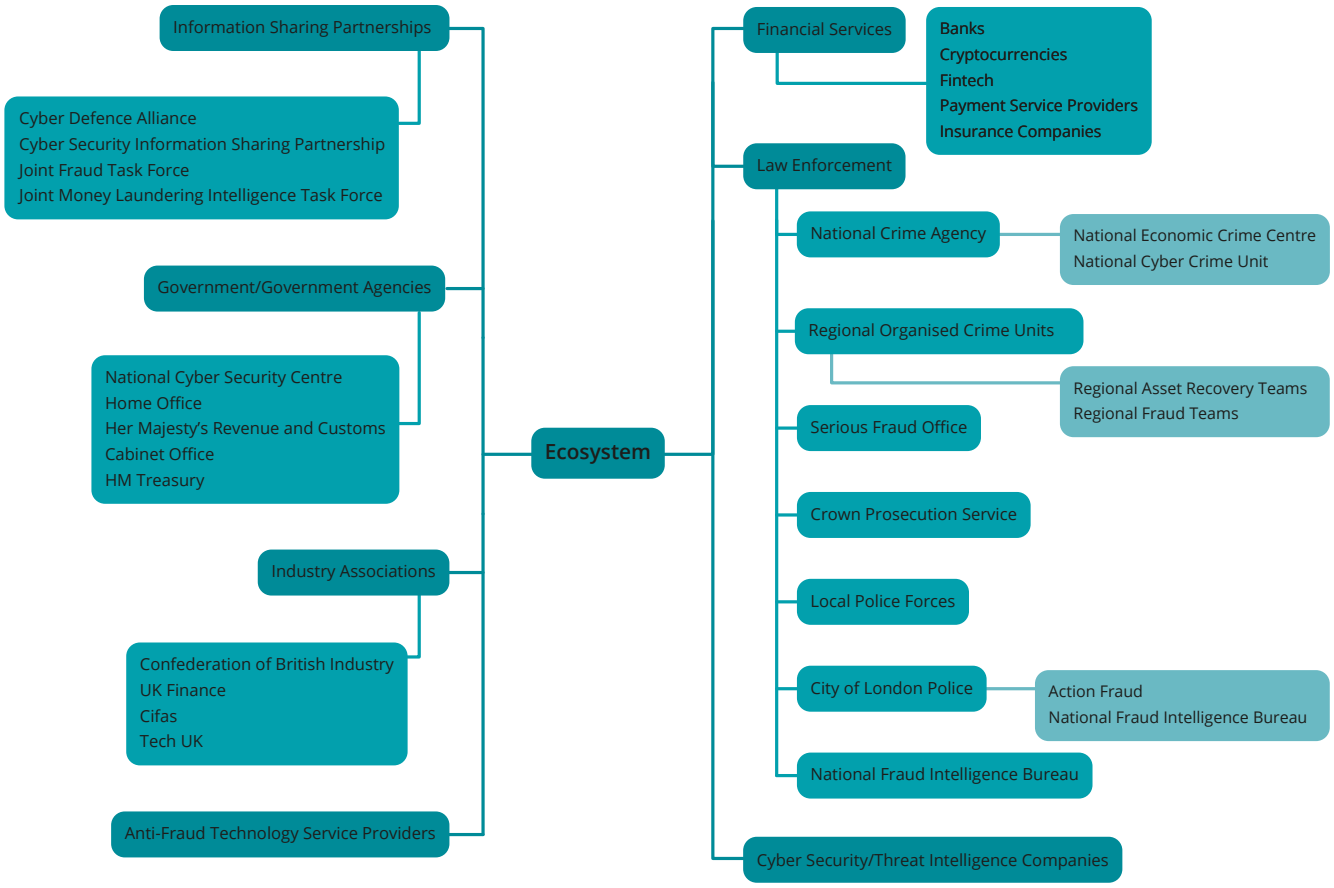
The current UK model to combat cyber fraud is part of a wider strategy to increase national cyber resilience, as articulated in the UK's National Cyber Security Strategy.[3] Data suggests that over half of all fraud in England and Wales is cyber enabled, meaning that a threat actor relies on some form of illicit computer network intrusion or disruption to commit the crime.[4] This type of fraud is a primary motivator for cyber attacks on all organisations, so should be high on the agenda for security teams and business leaders.[5] Meanwhile, the UK government faces increasing pressure to develop a more connected approach which considers the different stages of cyber fraud in conjunction with each other. This approach would require an implementation strategy which key stakeholders co-develop and have responsibility to execute.

From the cyber attack phase through to data exploitation and the cash-out phase, this paper explores the lifecycle of a successful attack to show the variety of challenges law enforcement and financial institutions face in preventing and responding to cyber fraud. This includes addressing the challenge that cyber fraud investigations will rarely lead to a judicial outcome. The next phase of the research will provide actionable recommendations to inform future policy discussions on reforming the UK response to cyber fraud. This will consist of: a research paper informed by a series of interviews with key experts and stakeholders; a questionnaire to be disseminated among a wide cross-section of the financial sector; and a set of workshops aimed at triangulating and validating the emergent research findings.

Figure 1 outlines the stakeholders involved in tackling cyber fraud in England and Wales. As such a large ecosystem has grown organically over time, confusion relating to specific roles and responsibilities to tackle the threat is inevitable. At the same time, there are few means of measuring the accountability of individual actors in this expansive fraud response ecosystem. Engaging across the ecosystem is vital to understanding where their responsibilities lie in accordance with the lifecycle of cyber fraud and how to incentivise further action.

3. The National Cyber Security Strategy is a high-level policy aimed at coordinating and providing strategic outcomes that enable the UK to increase its cyber resilience. As such, cybercrime is a part of the strategy. See HM Government, 'National Cyber Security Strategy 2016–2021', 2016, p. 48; Jamie Saunders, 'Tackling Cybercrime – The UK Response', *Journal of Cyber Policy* (Vol. 2, No. 1, 2017), p. 6.
4. Henry Rex, 'ONS Crime Stats: Fraud & Cyber Crime Still Dominate', TechUK, 19 July 2018, <https://www.techuk.org/insights/news/item/13518-ons-crime-stats-fraud-cyber-crime-still-dominate>, accessed 5 June 2020.
5. Intelligence Network, 'Our Vision for Tackling Cyber Fraud', June 2019, <https://content.baesystems.com/theintelligencenetwork/uk/topic-3-10FH-75777.html>, accessed 5 June 2020.

Figure 1: Cyber-Enabled Fraud Stakeholder Ecosystem



Source: Author generated.

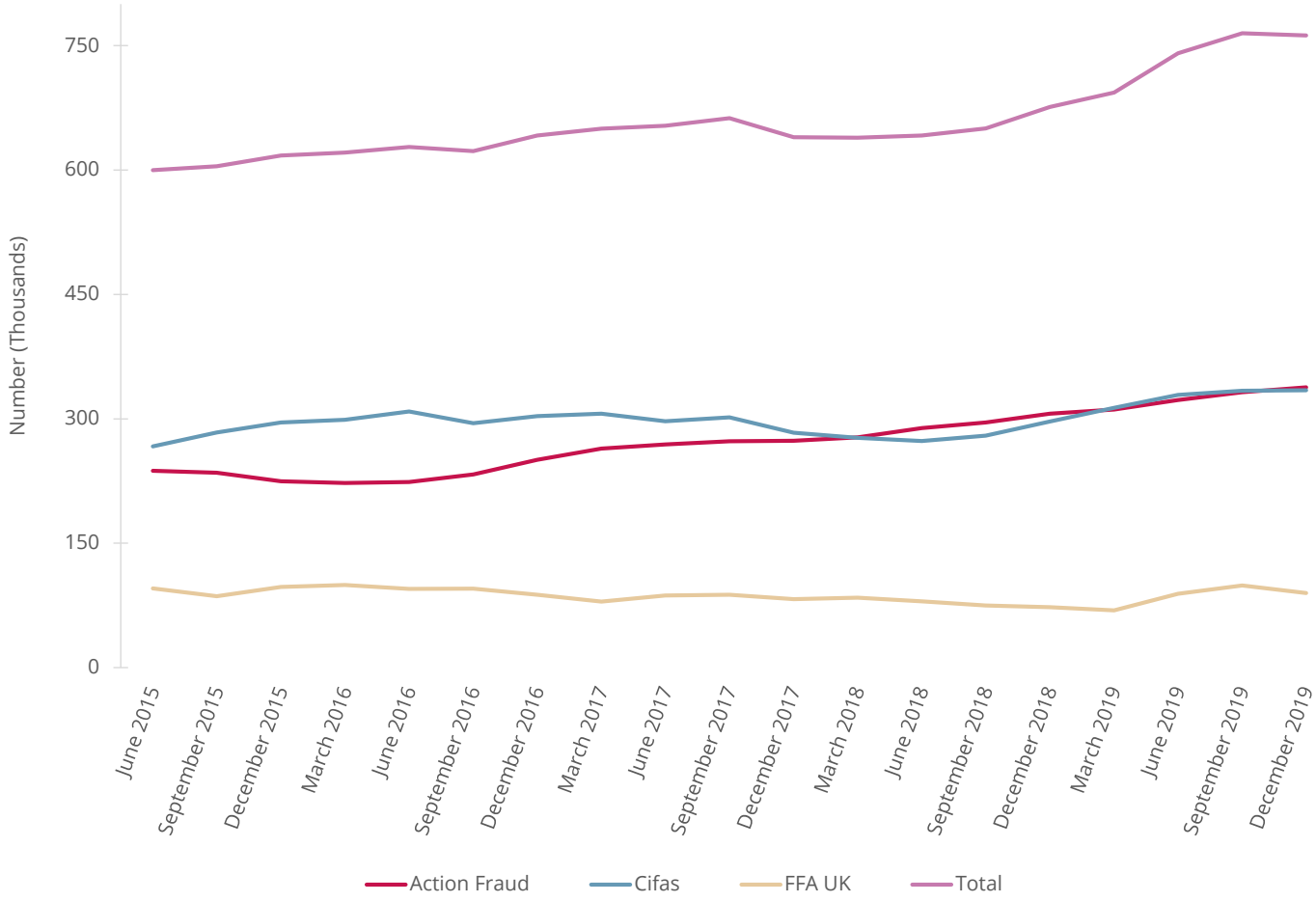
It is currently impossible to measure the true scale of cyber fraud in the UK. The majority of offences are never reported to authorities, and the statistics that are available often conflict due to the use of different definitions or interpretations of recorded data. These challenges notwithstanding, self-report figures in the Crime Survey for England and Wales provide perhaps the most representative indication of recent trends in cyber fraud offences.

As shown in Figure 2, total reported fraud increased from 639,457 in December 2017 to 762,266 in December 2019 – an increase of more than 19%. One factor contributing to this rise, which is often highlighted in various cybercrime threat assessments, is that there is a low barrier to entry for cyber-criminals due to the increasing availability of cybercrime as a service.[6] Brokers who provide specialist functions have become a key player in the cybercrime ecosystem.[7]

It is worth noting that there is some contention around whether these are increases in frauds or just a result of improvements in the reporting system or public awareness. It is unlikely that there is a conclusive answer, but recent research on public awareness and attitudes towards Action Fraud would cast some doubt on that idea.[8]

6. National Crime Agency (NCA), 'National Strategic Assessment of Serious and Organised Crime', 2020.
7. Maria Grazia Porcedda and David S Wall, 'Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk Hack', WACCO 2019: First Workshop on Attackers and Cyber-Crime Operations, June 2019, p. 8.
8. Laura Blakeborough and Sara Giro Correia, *The Scale and Nature of Fraud: A Review of the Evidence* (London: Home Office, 2019), p. 8.

Figure 2: Number of Reported Fraud Instances, 2015–19



Source: Adapted from Office of National Statistics, 'Crime in England and Wales Statistical Bulletins', last updated 23 April 2020.

THE THREAT FROM CYBER FRAUD

The challenges of reporting and measuring cyber fraud further add to the challenges faced by law enforcement agencies and financial institutions. Notably, the transnational nature of cyber fraud and distinctive features of the lifecycle of the crime present a number of challenges.

FRAUD AS A TRANSNATIONAL CRIME

Cyber fraud rarely only involves a single law enforcement jurisdiction.[9] To complicate the issue further, cybercrime spans national boundaries, with victims and offenders commonly located in different countries.[10] One of the most challenging features of cybercrime is the fact that while the internet enables global access to networks and data, law enforcement agencies and governments remain restricted by national boundaries. This has an impact on transnational investigations and cooperation, particularly at a time when longstanding UK foreign policy engagement is undergoing change.[11]

FRAUD AND THE CYBERCRIME ECOSYSTEM

Cyber fraud often involves several criminals with different areas of expertise, such as those responsible for launching cyber attacks or those tasked with 'cashing out' the proceeds of crime.[12] Consequently, law enforcement agencies and financial institutions need to call on a range of expertise to tackle cyber fraud. This inevitably requires significant resource investment. Law enforcement may try to track criminal activity at every level, to increase the risk of each stage of the crime for a criminal actor. However, as one actor or group is taken down, another often fills the void. This is due to the criminal forums and closed networks that allow cyber-criminals to work together with almost complete impunity and without any concerns relating to physical location.[13]

9. Michael Skidmore et al., *More Than Just a Number: Improving the Police Response to Victims of Fraud* (London: The Police Foundation, 2018), p. 24.
10. Carl Miller, 'British Police Are on the Brink of a Totally Avoidable Cybercrime Crisis', *WIRED*, 22 August 2018.
11. Zachary B Wolf and JoElla Carman, 'Here Are All the Treaties and Agreements Trump Has Abandoned', *CNN*, 1 February 2019.
12. National Cyber Security Centre (NCSC), 'Cyber Crime: Understanding the Online Business Model', 2017. In their paper, the NCSC outlines the different, highly specialised skillsets that are required, such as team leader, coder, network administrator, intrusion specialist, data miner and money specialist. For the purposes of this paper, we have replaced 'business model' with 'ecosystem' to reflect the contemporary literature on the topic, which mirrors this approach. See, for example, Stearns Broadhead, 'The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments', *Computer Law & Security Review* (Vol. 34, No. 6, 2018), pp. 1180–96.
13. UN Office on Drugs and Crime, 'Obstacles to Cybercrime Investigations', March 2019, <https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html>, accessed 25 June 2020.

It is convenient to consider three stages to the cyber fraud lifecycle. Together, these comprise the cybercrime ecosystem.[14]

Stage 1: Cyber Attacks and Data Theft

Box 1: Valuable Forms of Data

- Personal financial information (names, bank details and National Insurance numbers).
- Company accounts.
- Client databases.
- Intellectual property (for example, new company products or innovations).
- Detailed open source intelligence searching for personal information – including date of birth, names and family details – which is often accessible through social networking, dating and employment sites.

The National Crime Agency (NCA) estimates that 54% of all fraud cases involve the use of the internet to illegally obtain information about potential victims.[15] This is particularly relevant as the shift to remote working and the rapid digitalisation of organisations, accelerated by the ongoing coronavirus pandemic restrictions, increases the threat surface considerably. There has been an increase in attempted coronavirus-related intrusion methods as a result.[16] Generally, data theft arising from cyber intrusions is a global problem, and international borders are irrelevant to this type of crime.[17] For investigations to have any positive outcome, they require complex cross-border operations.

Cyber attacks, including those involving social engineering,[18] are inherently difficult to defend against. According to Kaspersky, 52% of businesses believe

14. The lifecycle of cyber fraud is a model that has previously been used. The authors' three stages are inspired by: 41st Parameter, 'Surveillance, Staging and the Fraud Lifecycle: Turning the Tables on Cyber Criminals', White Paper, 2014; David S Wall, 'How Big Data Feeds Big Crime', *Current History: A Journal of Contemporary World Affairs*, 1 January 2018, pp. 29–34; Porcedda and Wall, 'Cascade and Chain Effects in Big Data Cybercrime'.
15. NCA, 'National Strategic Assessment of Serious and Organised Crime'.
16. The NCSC warns of the increase in coronavirus-related scams, commonly in the form of phishing emails. See NCSC, 'UK and US Security Agencies Issue COVID-19 Cyber Threat Update', 8 April 2020, <https://www.ncsc.gov.uk/news/security-agencies-issue-covid-19-cyber-threat-update>, accessed 17 June 2020.
17. The Carnegie Endowment for International Peace has collated a useful timeline of all known cyber intrusions involving financial institutions across the globe. See Carnegie Endowment for International Peace, 'Timeline of Cyber Incidents Involving Financial Institutions', <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline>, accessed 17 June 2020.
18. Social engineering is one category of techniques used to penetrate a victim's device by attempting to convince them of, for example, an email's authenticity. The most common social engineering attack is phishing (the use of emails to convince a victim to click on a fake website or download a file which contains malware). For more details, see Kaspersky, 'What is Social Engineering?',

that the biggest weakness to their cyber security is their employees.[19] Phishing – including targeted spearphishing campaigns – is a common method used by criminals to gain access to a network, by encouraging a victim to click on a link or download a malicious file. In particular, business email compromise is the fastest-growing threat, especially for small businesses who typically have poor cyber security controls and awareness.[20] Organised criminal groups or individual opportunists employ a range of tools to conduct a technical attack – including the use of watering holes[21] – and exploit kits to scan a victim's computer for vulnerabilities, in order to deploy additional malware such as keyloggers.[22] These methods of attack are effective in exploiting the poor implementation of cyber security in many organisations.

Stage 2: Use of Stolen Data to Commit Fraud and/or Sale of the Stolen Data

Following the technical theft of data, cyber criminals will exploit harvested data in various ways to carry out fraud. Data is commonly sold via online criminal marketplaces on the dark web,[23] and criminals sell stolen data to other criminals who may commit 'secondary fraud'.[24] Tools such as automated vending carts (AVCs) allow datasets to be bought in bulk with cryptocurrencies. These datasets typically include credentials and passwords alongside financial information such as credit card details.[25]

Cyber attacks, including those involving social engineering, are inherently difficult to defend against

<https://usa.kaspersky.com/resource-center/definitions/social-engineering>, accessed 17 June 2020.

19. Kaspersky, 'The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within', <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>, accessed 5 June 2020.
20. NCA, 'National Strategic Assessment of Serious and Organised Crime'.
21. A watering hole is a site identified as frequently used by people within a given target organisation. The criminal inserts an 'exploit' into the website, which attempts to find vulnerabilities when a victim uses the website. This is a common method of deploying other malware. For more details, see Trend Micro, 'Watering Hole 101', 13 February 2013, <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/137/watering-hole-101>, accessed 5 June 2020.
22. A keylogger is a piece of malware that records every stroke of a device keyboard. They are commonly used to record username and passwords on a victim's device. For more details, see McAfee, 'What is a Keylogger?', 23 July 2013, <https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger/>, accessed 5 June 2020.
23. The dark web is a hidden area of the internet not accessible via standard browsers or search engines. It is commonly associated with criminal activity and uncensored marketplaces for illegal goods. Stolen data is openly bought and sold on dark web marketplaces. For more details, see Norton, 'How to Safely Access the Deep and Dark Webs', <https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html>, accessed 17 June 2020.
24. NCSC, 'Cyber Crime', p. 8.
25. Digital Shadows, 'Dark Web Monitoring: The Good, the Bad, and the Ugly', 11 September 2019, <https://www.digitalshadows.com/blog-and-research/dark-web-monitoring-the-good-the-bad-and-the-ugly/>, accessed 5 June 2020.

Enigma is one prominent marketplace for stolen data. In July 2019, it had 20,000 listings for sale, identifiable by the company the data was stolen from.[26] The financial sector, in particular, has been a regular target: research by Crowe UK and the University of Portsmouth found that of the top 50 UK brands, eight banking and finance organisations were affected by information trading on the dark web.[27] While other dark web marketplaces have been taken down, AVCs continue to thrive. However, law enforcement and cyber threat intelligence companies continue to monitor AVCs and data exploitation, as well as resale more generally.

It is also worth noting recent evidence which shows how forums on the surface web are used for the illicit trade of personal data.[28] While carrying a higher risk due to the relative lack of anonymity, these transactions are usually cheaper than on the dark web. Simple Google searches can lead users to forums where they can access postings of financial and personal information with a high level of detail.[29]

Stage 3: Money Laundering of the Proceeds of Cybercrime

The final stage of a cyber fraud operation is to channel stolen money through multiple bank accounts or via other payment methods. This serves the dual purpose of moving the funds away from the victim account while obscuring their criminal origin.

These flows of illegally obtained funds are often transnational in nature. The NCA assesses that overseas cybercrime groups, mostly from Russian-speaking countries, pose the greatest threat to the UK. However, these groups use UK-based money launderers or money mules as part of their cybercrime ecosystem.[30]

One challenge for both law enforcement and the financial sector is how to connect the various stages of the cybercrime ecosystem, so that interventions are made at the right stage with maximum impact. For example, it may be easier to investigate low-level UK-based money mules than high-level suspects based in hard-to-reach jurisdictions. However, the impact of a successful investigation into a money mule, including a beneficial judicial outcome, may be low. It may do little to reduce the incidence of cybercrime, and overseas organised cybercrime groups will likely recruit elsewhere.

---

26. Digital Shadows, 'A Growing Enigma: New AVC on the Block', 19 July 2019, <https://www.digitalshadows.com/blog-and-research/a-growing-enigma-new-avc-on-the-block/>, accessed 5 June 2020.
27. Jim Gee et al., 'The Dark Web: Bad for Business: Research into the Planning and Monetisation of Fraud and Cybercrime Against Organisations on the Dark Web', Crowe, 2018, p. 6.
28. Cifas, 'Fraudscape 2019', Report, June 2019, p. 8.
29. Cifas and Forensic Pathways, 'Wolves of the Internet: Where do Fraudsters Hunt for Data Online?', June 2018, p. 7.
30. NCA, 'National Strategic Assessment of Serious and Organised Crime', p. 46, para. 138.

CURRENT RESPONSES TO TACKLING CYBER FRAUD

The lifecycle approach to cyber fraud reflects the criminal business model. However, the question of whether or not the current response to tackling cyber fraud reflects the criminal business model effectively remains. Notably, the number of stakeholders in the ecosystem that are involved in each stage creates a complex mix of interventions, as shown in Figure 1.

THREAT INTELLIGENCE AND TECHNICAL INTERVENTIONS

Cyber threat intelligence is a growing industry.[31] Financial institutions use it to pre-emptively defend their networks, and in doing so, they maintain some of the highest expenditure on cyber security of any industry.[32] Cyber threat intelligence is not just an internal function of financial institutions and law enforcement – there is a cyber security industry built to provide threat intelligence and an understanding of the threat landscape. Despite various intelligence-sharing partnerships (see Figure 1), one challenge is balancing the legitimate commercial incentives of the threat intelligence industry with whole-of-society incentives that create a more open information-sharing environment between government, law enforcement and industry.

There are many examples of partnerships between law enforcement and industry carrying out technical interventions such as botnet takedowns.[33] One barrier to success relates to the legal and regulatory environment in which these operations are carried out, including the jurisdictions where malicious infrastructure is located.[34] This inevitably inhibits law enforcement operations when infrastructure is located within an uncooperative state. In addition, it is unclear to what extent private sector organisations should carry out these types of cybercrime interventions unilaterally. The recent

31. Markets and Markets, 'Threat Intelligence Market by Solution (Threat Intelligence Platforms, SIEM, IAM, SVM, Risk and Compliance Management, Incident Forensics), Service (Managed, Professional), Deployment Mode, Organization Size, Vertical, and Region – Global Forecast to 2023', November 2018, <https://www.marketsandmarkets.com/Market-Reports/threat-intelligence-security-market-150715995.html>, accessed 17 June 2020.
32. *Business Wire*, 'New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services', 16 October 2019.
33. A bot is a compromised ('robot' or 'zombie') computer that criminals can control remotely. A botnet is a networked collection of compromised machines. Botnets can easily contain over 10,000 compromised computers.
34. A botnet alone is not necessarily linked to malware or malicious intent. Some botnets exist for user experience. A malicious botnet gains access to a device and adds it to the criminal's master computer in their network to control the device when needed to send requests to a targeted network. It may also be used to distribute spam to other users. For more details, see Norton, 'What is a Botnet?', <https://uk.norton.com/internetsecurity-malware-what-is-a-botnet.html>, accessed 5 June 2020.

takedown of the Necurs botnet orchestrated by Microsoft is one example of an initiative led by the private sector, in cooperation with government and law enforcement. Microsoft worked with internet service providers, domain registrars, government computer emergency response teams and law enforcement agencies in Mexico, Colombia, Taiwan and more.[35]

Some believe that governments do not have the capacity to lead on botnet takedowns and that the private sector should assume more responsibility by coming together to support a centre of excellence on botnet takedowns, while pressuring companies who inadvertently enable the activity.[36] In the UK, the primary law relating to this activity is the Computer Misuse Act 1990 (CMA).[37] Some argue that the CMA is no longer fit for purpose,[38] not least because it exposes law enforcement and cyber security professionals to prosecution as they seek to identify and mitigate vulnerabilities. Others conversely argue that there are more pressing issues linked to incentivising better cyber security and addressing the skills gap, rather than providing citizens with the legal authority to conduct intrusive cyber operations.[39] In the UK, there would be legal and ethical concerns if private sector organisations were to conduct technical interventions without the involvement of government and law enforcement.

Finally, there is a gap in understanding the impact of botnet takedowns and other technical interventions. In some cases, they have a short-term soothing effect and cyber-criminals quickly set up new malicious infrastructure.[40] More needs to be done to produce better metrics on the impact of technical cybercrime operations, including an understanding of how operations are prioritised and the resource required.

35. Gareth Corfield, 'Microsoft Nukes 9 Million-Strong Necurs Botnet After Unpicking Domain Name-Generating Algorithm', *The Register*, 11 March 2020.
36. Robert K Knake, 'To Get to Zero Botnets, Don't Wait for Governments to Lead', Council on Foreign Relations, 26 November 2018, <https://www.cfr.org/blog/get-zero-botnets-dont-wait-governments-lead>, accessed 5 June 2020; Karine K E Silva, 'How Industry Can Help Us Fight Against Botnets: Notes on Regulating Private-Sector Intervention', *International Review of Law, Computers & Technology* (Vol. 31, No. 1, 2017), pp. 105–30.
37. Computer Misuse Act 1990 (UK).
38. Owen Bowcott, 'Cybercrime Laws Need Urgent Reform to Protect UK, Says Report', *The Guardian*, 22 January 2020; Criminal Law Reform Now Network, 'Reforming the Computer Misuse Act 1990', 2020.
39. Daniel Pedley et al., 'Cyber Security Skills in the UK Labour Market 2020', Findings Report, Department for Digital, Culture, Media and Sport, March 2020; RedSeal, 'UK Business at Risk as Cyber Skills Gap Reaches Breaking Point', 27 November 2019, <https://www.redseal.net/uk-business-at-risk-as-cyber-skills-gap-reaches-breaking-point/>, accessed 5 June 2020.
40. Shane Schick, 'Dridex Trojan Remains a Risk Even Following Takedown Operation and FBI Arrest', Security Intelligence, 19 October 2015, <https://securityintelligence.com/news/dridex-trojan-remains-a-risk-even-following-takedown-operation-and-fbi-arrest/>, accessed 5 June 2020.

THE ROLE OF THE FINANCIAL SECTOR

Financial institutions are frequently an attractive target and victim of cyber attacks because of the value of their data. This poses a fundamental risk to the UK government's ambition of being the safest place in the world to conduct business online.[41] When customers entrust their data to financial institutions, there is a reciprocal responsibility to establish mutual trust in the event of a breach. Consumers need to feel that their experience is being taken as seriously as with more traditional forms of crime such as robbery or burglary. Discerning how these modern, complex crime types are affecting consumers' behaviours and expectations of their bank is crucial in achieving fair distribution of responsibility.

The increasing digitalisation of services and products in the financial sector, while creating efficiencies, also brings new vulnerabilities by increasing the attack surface.[42] Alongside the rise in working from home following the outbreak of coronavirus, developments such as 'bring your own device' to work, mobile payments and cloud storage have enabled information security breaches to become ubiquitous.[43] At the same time, financial institutions spend three times more on cyber security than other sectors.[44] UK financial institutions also spend a further £5 billion annually to comply with economic crime regulations.[45] Adding to the costs associated with cyber fraud prevention, breaches can be significantly damaging for financial institutions both in terms of the financial cost of reimbursing customers for any stolen money and the reputational damage caused by loss of consumer trust.[46]

41. HM Government, 'Internet Safety Strategy – Green Paper', October 2017.
42. Laura Noonan, 'Advancing Bank Technology "Broadens Hack Attack Surface"', *Financial Times*, 22 March 2020.
43. Euromoney, 'Seeing off the Cybercriminals', April 2020, <https://www.euromoney.com/article/b1lbk9482pkcvs/seeing-off-the-cybercriminals>, accessed 2 July 2020. In this article, Caixabank explains the cyber security threat landscape from its perspective, including elaborating on banking infrastructure vulnerabilities. It specifically draws attention to the issue of scalability for mobile banking infrastructure, which is an issue as many customers convert to mobile banking. See also ITPro, 'Cloud Cyber Attacks up Seven-Fold During Coronavirus Pandemic', 28 May 2020, <https://www.itpro.co.uk/cloud/cloud-security/355815/cloud-cyber-attacks-increased-seven-fold-over-coronavirus-pandemic>, accessed 2 July 2020. The cloud has been increasingly targeted throughout the pandemic, while many companies switch to cloud services. See also Accenture Security, 'Cybersecurity Risks Related to COVID-19', 4 June 2020, <https://acn-marketing-blog.accenture.com/wp-content/uploads/2020/04/Accenture_SITREP_COVID-19_20200604_v10.pdf>, accessed 2 July 2020.
44. UK Finance and KPMG, 'Staying Ahead of Cyber Crime', April 2018, p. 4.
45. *Ibid.*, p. 12.
46. Kevin Peachey, 'Scam Victims to be Refunded by Banks', *BBC News*, 28 May 2019; EY, 'Cybercrime. What Does the Most Damage, Losing Data or Trust?', 9 April 2019.

For larger organisations, risk-management processes for cyber security may be complex.[47] One challenge for financial institutions is to manage security in 'controlled and audited' environments 'delivered at the pace that … verification and accounting process allows'.[48] This can be particularly troublesome for banks who may have legacy infrastructure to protect and audit which contains vulnerabilities that cyber-criminals can exploit.

Meanwhile, financial institutions may not have the appropriate internal structures in place to mitigate risk linked to the various stages of the cybercrime ecosystem. Departments that deal with cyber security may be siloed from departments that deal with fraud, even though the investigation concerns the same criminal group. This challenge can adversely impact how financial institutions work together to investigate cybercrime.[49] Until these structural challenges are resolved, existing interventions will have little impact on the overall volume of cyber fraud.

Financial institutions are frequently an attractive target and victim of cyber attacks

DISRUPTING ILLICIT MONEY FLOWS

At stage three of the cybercrime ecosystem, there are three key methods used to cash out the proceeds. First, the use of money mule accounts.[50] On behalf of a criminal, mules conduct rapid transfers across a number of accounts to move the proceeds of banking Trojans such as Dridex,[51] which allegedly generated $100 million in criminal income.[52] Second, it has long been reported that cyber fraudsters set up corporate accounts[53] to use for

47. Financial institutions also have many third-party networks and vendors that connect to the bank to provide services to customers, such as SWIFT, the global payments service provider. In the case of a breach on Bangladesh Bank in 2016, SWIFT was an attack surface that was exploited. See UK Finance and KPMG, 'Staying Ahead of Cyber Crime', p. 6.
48. UK Finance and KPMG, 'Staying Ahead of Cyber Crime', p. 7.
49. Michael Levi et al., 'Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research', *Crime, Law, and Social Change* (Vol. 67, No. 1, 2017), p. 80.
50. 'Mule' is a common term for an individual who wittingly or unwittingly transfers money or, in some instances, goods. See Krebs on Security, 'How Cybercriminals are Weathering COVID-19', 30 April 2020, <https://krebsonsecurity.com/2020/04/how-cybercriminals-are-weathering-covid-19/>, accessed 5 June 2020.
51. Eight individuals involved in laundering Dridex proceeds were sentenced to prison terms in the UK. See NCA, 'International Law Enforcement Operation Exposes the World's Most Harmful Cyber Crime Group', 5 December 2019.
52. US Department of Justice, 'Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware', press release 19-1346, 5 December 2019.
53. An FBI affidavit submitted in March 2020 details how the QQAAZZ cyber-criminal group allegedly used 'dozens of shell companies' with bank accounts in, among other countries, the UK to launder the proceeds of cyber-enabled fraud. See

particularly large transfers.[54] Finally, criminals use virtual assets. A cyber fraudster can either criminally obtain virtual assets – such as through a cryptocurrency scam[55] – or purchase them to hide their financial trail.[56] Of these modi operandi, money mules are of the most direct concern to the financial sector.

Box 2: Money Mule Accounts

The utility of a money mule lies in supplying a bank account that a criminal can use to move funds. Instead of recruiting a money mule, a criminal can obtain access to a bank account in other ways, such as by opening multiple accounts thanks to a corrupt bank insider[57] or hacking an account. From a financial institution's perspective, it therefore makes sense to speak of 'money mule accounts', or accounts that are used for criminal purposes on behalf of someone other than ostensible account holders.

Prosecuting low-level mules (sometimes ironically referred to as the 'whack-a-mule' game) is not sufficient to meaningfully reduce the impact of cybercrime on the UK. Of more importance are money mule recruiters, also known as mule herders. Since they can be based overseas and thus be physically out of the reach of UK law enforcement, taking action against them can run into challenges similar to those that beset all cybercrime investigations.

There are some well-documented examples of good practice in money mule disruption that could be carried over into any new model to tackle cybercrime.[58] The first of these is the analysis of a broad range of data points to identify linked accounts. Indications that purportedly unrelated accounts have been opened, or are being used by, the same individual or group are a sign of possible money mule activity. Such links can sometimes be gleaned by identifying the digital footprints of customers. Doing so effectively may rely on the expertise – and, occasionally, data – held by financial institutions'

US v Maksim Boiko, US District Court for the Western District of Pennsylvania, Affidavit in Support of Complaint, 27 March 2020, p. 11.

54. See, for example, Max Goncharov, 'Russian Underground 2.0', Research Paper, Trend Micro, 2015, p. 11.
55. See, for example, Chainalysis, 'The 2020 State of Crypto Crime: Everything You Need to Know About Darknet Markets, Exchange Hacks, Money Laundering and More', January 2020, pp. 16–29.
56. US v Maksim Boiko, US District Court for the Western District of Pennsylvania, Affidavit in Support of Complaint, 27 March 2020, p. 12.
57. For instance, this is how part of the Dridex proceeds were laundered in the UK. See Phil Muncaster, 'Barclays Bank Insider Sentenced for Role in Dridex Plot', *Infosecurity*, 15 December 2017, <https://www.infosecurity-magazine.com/news/barclays-bank-insider-sentenced/>, accessed 2 July 2020.
58. See Anton Moiseienko and Olivier Kraft, 'From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime', *RUSI Occasional Papers* (November 2018), pp. 65–66.

cyber security departments, as well as on their effective collaborations with financial crime teams.

A second strategy is information sharing among companies. There are at least two types of information sharing that can contribute to money mule disruption. On the one hand, there is the sharing of information on cyber threat actors and their modus operandi, which is undertaken by groups such as the Cyber Defence Alliance in the UK and the National Cyber-Forensics and Training Alliance in the US. It can help identify cyber security vulnerabilities, better understand the true scale of a given threat actor's operations and detect money mule networks. On the other hand, there is the sharing of information on the flow of stolen funds. Tracing the flow of funds that originate from a known fraudulent transfer, so that accounts involved can be swiftly identified and frozen, is the principle behind the Mule Insights Tactical Solution, a technological platform used by some UK banks (12 banks as of its launch in September 2018).[59]

Finally, education through public awareness campaigns – such as those run by UK Finance and Cifas – aims to reduce the likelihood of people being duped into acting as money mules in the first place.[60]

BARRIERS TO AN EFFECTIVE RESPONSE

This paper categorises the barriers to reducing the impact of cybercrime into three broad categories: reporting; enforcement; and investigation.

Table 1: Criminal Justice Response to Cyber-Enabled Control

	Reporting	Investigation	Enforcement
Key Barriers	Reputational risk to organisations reporting breaches	Volume of cyber-enabled fraud relative to investigation capacity	Reliance on other countries' cooperation
	Perceived lack of investigation and enforcement	Incomplete threat picture leading to prioritisation challenges	Complex and time-consuming nature of investigations – attribution and digital forensics
	Levels and funding of training of Action Fraud	Levels of staffing and pay scales in cyber security skills	Differences in legislative frameworks
		Inconsistent recording of investigation outcomes and circulation of 'best practice'	Post-Brexit diplomatic uncertainty and partnerships

Source: Author generated.

59. House of Commons Treasury Committee, 'Economic Crime: Consumer View', 22 October 2019, p. 31, para. 126.
60. See, for example, UK Finance and Cifas, 'Don't be Fooled', <https://www.moneymules.co.uk/>, accessed 5 June 2020.

REPORTING CHALLENGES

The cyber fraud reporting process requires significant review and reform. This is important for two main reasons. First, the reporting centre – Action Fraud in the UK – is responsible for recording all information pertaining to a potential investigation. If there are failings in the way this information is captured, it will affect how serious the case is perceived to be when it is passed onto the National Fraud Intelligence Bureau (NFIB),[61] and then the relevant police force. Second, a reporting centre is likely to be the victim's first point of contact in the immediate moments following a fraud, and if this period is not handled with the required sensitivity, it risks damaging individual victims' confidence in the system as a whole.

Much has been written on how the funding and training of Action Fraud staff has affected competency in handling complaints.[62] This was the basis for Craig Mackey and Jerry Savill's report on Action Fraud this year, although it remains a unique service by global standards.

From the perspective of the victim, however, there are notable barriers to engaging with the reporting process. One of these is the reputational risk associated with being seen as a company with weak cyber security and fraud prevention infrastructures – an analysis of share price fluctuations following a data breach revealed that finance companies that leak highly sensitive credit card information see the largest drops in share price performance in the medium term.[63] A second, potentially more serious, disincentive to

61. Action Fraud and the National Fraud Intelligence Bureau (NFIB) are both housed in the City of London police force. Due to the volume of reports that Action Fraud receives, and the fact that not all reports will contain viable leads for investigation, it is not feasible for NFIB staff to look at every crime report. Two automated approaches are used to identify the cases which are theoretically most likely to have viable lines of enquiry. One is a 'scoring matrix', which automatically scores crimes based on the presence or absence of certain information. The other is 'manual review criteria' based on elements such as level of monetary loss or type of crime reported, which helps to identify potentially more severe victim impact and develop an intelligence picture to support collaborative activity. If either of these criteria are met, the case is reviewed by an NFIB crime reviewer, who then decides whether to send the case to a local police force for further investigation.
62. See, for example, Faye Lipson, 'Exclusive: Scam Victims Ignored by Police Fraud Reporting System', *Which?*, 27 September 2019; Stephen Little, 'Scam Victims Mocked and Deliberately Misled by Action Fraud While Police Fail to Catch Fraudsters', Moneywise, 15 August 2019; Craig Mackey and Jerry Savill, 'A Review of the National "Lead Force" Responsibilities of the City of London Police and the Effectiveness of Investigations in the UK', HM Government, 24 January 2020; Angie Scholes, *The Scale and Drivers of Attrition in Reported Fraud and Cyber Crime*, Home Office, Research Report 97 (London: The Stationery Office, 2018).
63. Paul Bischoff, 'How Data Breaches Affect Stock Market Share Prices', Comparitech, 20 April 2020, <https://www.comparitech.com/blog/information-

reporting is the perception that the subsequent stages of investigation and enforcement will only prove to be a further drain on time and resources.

In what can quickly become a self-fulfilling prophecy, if victims believe that there is a track record of ineffective law enforcement response to large-scale cyber frauds, they may scale back their willingness to devote resources to cooperation. In turn, this lowers the quality of information that law enforcement have to work with and the chances of successful future investigations. Aligning incentives to report fraud when it happens is a significant policy challenge and will have a bearing on how and whether justice is dispensed in the cyber world. It is worth noting how changes in the legal infrastructure, such as the introduction of the General Data Protection Regulation (GDPR) in 2018, can serve as a tool to alter those incentives.

INVESTIGATION CHALLENGES

The sheer volume of cyber fraud far exceeds the relative in-house capacity that law enforcement possesses.[64] Less than 1% of UK policing's total workforce is involved in fraud investigation,[65] and their ability to accurately set staffing levels in response to demand forecasts is limited.[66] In particular, policing must compete with staffing demands and competitive pay scales to attract people with cyber security skills.[67] Meanwhile, there is little differentiation in the official statistics between frauds in terms of seriousness, complexity or harm, making it difficult to measure the efficiency of resource use across forces.[68] These limitations could to some extent be mitigated with a clear, universal set of prioritisation principles applicable to cases of cyber fraud used across law enforcement. But this has not yet materialised, even though there are some prioritisation processes in place for the purposes of immediate response to cyber attacks. This increases the risk that victims in different geographic locations will receive different treatment for the same type of crime.

Even for those victims whose cases are prioritised, there are some key limitations to investigative capacity. One persistent problem is the lack of information on perpetrator tradecraft – namely, whether they are specialising

security/data-breach-share-price-analysis/>, accessed 5 June 2020.

64. Saunders, 'Tackling Cybercrime', p. 9; House of Commons Home Affairs Committee, 'Policing for the Future: Tenth Report of Session 2017–19', HC 515, October 2018, p. 27.
65. Mackey and Savill, 'A Review of the National "Lead Force" Responsibilities of the City of London Police and the Effectiveness of Investigations in the UK', p. 6.
66. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), *Cyber: Keep the Light On – An Inspection of the Police Response to Cyber-Dependent Crime* (London: HMICFRS, 2019), p. 12.
67. Emma Woollacott, 'Why Police Need the Skills to Counter Cybercrime', *Raconteur*, 27 September 2019, <https://www.raconteur.net/technology/police-skills-cybercrime>, accessed 26 June 2020.
68. Skidmore et al., *More Than Just a Number*, p. 8.

in some frauds more than others, sharing best practice, attack mechanisms and victim lists in the process.[69] Closely related to this, there is limited knowledge about the extent to which organised crime groups (OCGs) have orchestrated an attack. In 2019, for example, a publication by HMICFRS (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services) found national inconsistencies in the standards used for OCG mapping of specialist cyber threats.[70] The accumulation of these factors, alongside the fact that NFIB is afforded limited influence over what local action is taken to progress cases, can lead to notable differences in the way each force analyses the information they receive. This, in turn, affects the extent to which they meet central performance indicators.[71] This points to a broader unintended consequence of consolidating crime recording and analysis in the UK without a national fraud policing strategy: a disparity between what is known about fraud at the national level and what is done about it on the ground.[72]

When local police forces do conclude investigations, there is another problem regarding the recording of those outcomes. The various steps of the referral process commonly lead to a failure to refer important information back to NFIB and other law enforcement actors.[73] This includes the circulation of best practice and 'what works', which HMICFRS found does not take place in a structured way outside national agencies.[74] The more intelligence that slips through the cracks, the more difficult it becomes to coherently map the relevant cyber threat actors and mechanisms, as well as understand the different stages of the victim experience.

Box 3: Relevant Legislation

- Theft Act (1968, 1978).
- Forgery and Counterfeiting Act (1981).
- Police and Criminal Evidence Act (1984).
- Malicious Communications Act (1988).
- Computer Misuse Act (1990).
- Proceeds of Crime Act (2002).
- Serious Organised Crime and Police Act (2005).
- Fraud Act (2006).
- Data Protection Act (2018).

69. Levi et al., 'Cyberfraud and the Implications for Effective Risk-Based Responses', p. 89.
70. HMICFRS, *Cyber*, p. 10.
71. *Ibid.*, p. 9.
72. Michael Skidmore, Janice Goldstraw-White and Martin Gill, 'Understanding the Police Response to Fraud: The Challenges in Configuring a Response to a Low-Priority Crime on the Rise', *Public Money & Management* (Vol. 40, No. 5, 2020), p. 379.
73. Ruth Crocker et al., 'The Impact of Organised Crime in Local Communities', June 2017, p. 68.
74. HMICFRS, *Fraud: Time to Choose – An Inspection of the Police Response to Fraud* (London: HMICFRS, 2019), p. 7.

ENFORCEMENT CHALLENGES

The very nature of cyber fraud means that bringing perpetrators to justice is often reliant on effective cooperation with other jurisdictions and having the capability to identify the attacker. Attribution can be problematic because of the difficulty of establishing physical locations of perpetrators and electronic evidence, which requires significant digital forensics resources.[75] Unsurprisingly, this has knock-on effects for the likelihood of retrieving stolen money and therefore on deterring similar future crimes. Even when this information can be gathered, there are sometimes critical differences in the respective national legal frameworks which cause costly delays, even at the EU level.[76]

One challenge is how to harmonise existing operational processes, such as forensic-technical standards for exchanging electronic evidence with law enforcement agencies, which can offer valuable intelligence against some of the most sophisticated cyber-criminal infrastructures. At a more fundamental level, UK law enforcement may run into difficulties when working on a case involving countries that do not have comparable legislation to appropriately prosecute perpetrators of fraud.[77] This is linked to a broader debate over whether the mutual legal assistance process is agile enough to mitigate those obstacles.[78] Nonetheless, in June 2020, Europol launched the European Financial and Economic Crime Centre 'to promote the systematic use of financial investigations'. There will be an increased expectation on the UK to find ways to benefit from such new initiatives in the context of its exit from the EU.[79]

It is important to note that, domestically, one of the issues that is besetting policing is that part of the fraud offence is a computer misuse crime and the other is an economic crime. These are subject to different bodies of law and also the responsibilities of different police agencies. This means that

75. Europol and Eurojust Public Information, 'Common Challenges in Combating Cybercrime', Joint Report, June 2019, p. 13; Lily Hay Newman, 'Hacker Lexicon: What is the Attribution Problem?', *WIRED*, 24 December 2016.
76. Europol and Eurojust Public Information, 'Common Challenges in Combating Cybercrime', p. 14.
77. Tiggey May and Bina Bhardwa, *Organised Crime Groups Involved in Fraud* (London: Palgrave Macmillan, 2018), p. 76.
78. See CPS, 'Cybercrime – Prosecution Guidance', last updated 26 September 2019, <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>, accessed 5 June 2020. Mutual legal assistance is a method of cooperation between states for obtaining assistance in the investigation or prosecution of criminal offences. It is generally used for obtaining material that cannot be obtained on a police cooperation basis, particularly enquiries that require coercive means. Requests are made by a formal international letter of request, usually on the basis of a bilateral treaty or multilateral convention.
79. Europol, 'Europol Launches the European Financial and Economic Crime Centre', press release, 5 June 2020.

even if current laws are capable of dealing with the crime, their effective enforcement remains a significant challenge.

CONCLUSIONS AND POLICY QUESTIONS

Existing structures to tackle cyber fraud have not delivered the law enforcement outcomes that are needed. There is, therefore, a need to reassess the UK's current responses to cyber fraud to confront these shortcomings in a proactive and ambitious manner. This paper outlines some of the major reporting, investigation and enforcement challenges in tackling cyber fraud in the UK, by understanding the cyber fraud lifecycle and how it supports the cybercrime ecosystem.

The primary research for this project analyses in detail how law enforcement agencies and financial institutions should define their long-term roles and responsibilities in tackling cyber fraud. Full recommendations on how to do this will be set out in a forthcoming research paper in 2021 that will propose a new roadmap for tackling the threat from cyber fraud to the UK over the next decade and beyond.

The following policy questions are applicable to different stakeholders and should aid in signalling areas where each relevant actor has a specific role to play.

POLICYMAKERS

- How should the disparity between a global internet and a national/local law enforcement model be reconciled? What does this mean for models of transnational investigations and cooperation between jurisdictions with different priorities?
- To what extent is existing legislation appropriate to reducing cybercrime? Is there new regulation which could incentivise more proactive stakeholder action?
- Who should lead on the prevention work that safeguards individuals who may become involved in cybercrime?
- What is a realistic balance between investing in cyber security versus investigating and pursuing the perpetrators of cyber attacks?

LAW ENFORCEMENT

- What is the essential role for law enforcement in tackling cyber fraud?
- How should mechanisms for cybercrime reporting be reformed?
- Where are the examples of best practice and how can these be captured and disseminated in a more structured way?
- What can be done to start accurately quantifying the problem of cyber fraud? What metrics should be used to measure the effectiveness of any new model to reduce cyber fraud?

FINANCIAL INSTITUTIONS

- How could the financial sector more effectively contribute to the national effort to reduce cyber fraud over the next decade and beyond? How could this be incentivised?

PRIVATE SECTOR SECURITY INDUSTRY

- What is the impact of technical interventions and how could the current collaborative model be improved?
- What is the future of information-sharing utilities in the industry? How can they be made more mainstream and less ad hoc?

A comprehensive review and reform of the UK's response to cyber fraud is now essential to safeguard the country's future economic security and prosperity.

ABOUT THE AUTHORS

Sneha Dawda is a Research Analyst in RUSI's cyber security research programme. She specialises in national cyber security strategies, internet governance, critical national infrastructure vulnerabilities and cybercrime.

Ardi Janjeva is a Research Analyst at RUSI. His research currently spans numerous areas within organised crime and national security, including the application of emerging technologies for national security and law enforcement, intellectual property crime and counterfeiting, and cyber-enabled fraud.

Anton Moiseienko is a Research Fellow at RUSI's Centre for Financial Crime and Security Studies. His current and recent research covers a range of financial crime issues, including money laundering via online businesses, corruption in the UK and overseas, the intersection between cybercrime and money laundering, and financial crime risks posed by free trade zones.

This paper forms part of a research project sponsored by Huntswood. It precedes a RUSI research paper due for publication in early 2021, which will provide actionable policy recommendations based on in-depth primary research with law enforcement agencies, financial institutions and other key stakeholders.

About RUSI

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 189 years.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

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)