RUSI
Royal United Services Institute
for Defence and Security Studies

HUNTSWOOD

Occasional Paper

The UK's Response to Cyber Fraud

A Strategic Vision

Sneha Dawda, Ardi Janjeva and Anton Moiseienko

The UK's Response to Cyber Fraud

A Strategic Vision

Sneha Dawda, Ardi Janjeva and Anton Moiseienko

RUSI Occasional Paper, February 2021

Royal United Services Institute
for Defence and Security Studies

190 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 190 years.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution to which the authors are or were affiliated.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, February 2021. ISSN 2397-0286 (Online).

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 authors are grateful to Lord David Brownlow CVO DL and Huntswood for funding this paper and for their support throughout the research process. Lord Brownlow believes that the global pandemic and our shift to 'online everything' has expanded and accelerated the reach of cyber criminals and runs the risk of harming individuals, families and communities and undermining UK prosperity.

A great deal of thanks must go to Mike Peckham and Stephen Head of Gadhia Consultants for their enduring support and hard work that has contributed to this paper.

The authors would also like to thank Victoria Baines and Alix Newbold for their feedback and support, and for peer reviewing with such due diligence and sage advice.

A huge thank you to the Steering Committee that helped to shape and guide this project, which included Lord Brownlow, Oz Alashe, Victoria Wang, James Thomson, Oliver Bolton, Lord Hogan-Howe and Ben Russell.

Thank you to the comprehensive RUSI team that helped to guide and shape this paper. Conrad Prince, James Sullivan, Alexander Babuta and Tom Keatinge all deserve recognition for their support and edits. Particular thanks must go to Alexander Babuta for his brilliant work on the survey component of the methodology.

A final thank you to the participants of this research, to all those who very kindly gave up their time to participate in interviews and workshops when 2020 was challenging us all. Every single interview contributed greatly to the authors' thinking and synthesis of findings, and your responses to the survey truly make this a unique research paper.

Forewords

The Rt Hon Sir John Hayes MP

Member of the Intelligence and Security Committee of Parliament

'THE UK'S RESPONSE to Cyber Fraud: A Strategic Approach' provides clear, thorough and thoughtful analysis on how the UK should tackle cyber fraud, backed up by 12 detailed recommendations.

Technology has enabled freedom of information, revolutionised the workplace and, most recently, supported the UK's response to the coronavirus pandemic.

Despite such great benefits, society is increasingly impacted by cybercrime. Cybercrime is not only a threat to national prosperity and economic security, but, on a deeper level, it undermines our trust in technology. Cybercriminals use this doubt, uncertainty and fear to prey upon victims, costing the UK economy millions of pounds a year. And it is not just multinational corporations that fall victim to cyber fraud. Fraud is now the form of crime that British citizens are most likely to directly experience, making victims of individuals, families and small businesses.

Notable among the paper's 12 recommendations is the call for a whole-of-society approach to tackle cyber fraud, including a stronger relationship between law enforcement agencies and the financial services. In particular, I want to champion better information sharing among partners, and see victims prioritised through the allocation of further funding to the National Economic Crime Victim Care Unit.

Similarly, to ensure that we have the best and the brightest working for the common good against cybercriminals, the government must urgently consider innovative ways to equip law enforcement with more cyber specialists.

The consistent application of well-defined policy, supported by enhanced skills, is essential to enable law enforcement to stay ahead of criminals who seek to undermine the prosperity of the UK, ruining lives and livelihoods. I welcome this seminal RUSI paper as we strive for a safer digital society. ■

Commander Stephen Head (Retd)

Senior Partner, Gadhia Consultants and former National Coordinator for Policing Economic Crime

LIKE SO MANY of us, I have seen first-hand the misery caused by crime, particularly from fraud, to individuals, families and to our communities. In my time as the UK's first National Coordinator for Policing Economic Crime, I was particularly conscious that, even then, there were still people who considered fraud a victimless crime and just how important it was for us all to counter that myth and demonstrate the very real harm that this crime continues to inflict on the UK. The research presented in this paper highlights just how prevalent cyber-enabled fraud has become, touching every single one of us in some way. Although it is very clear this is a truly global issue, this paper demonstrates how its impact is felt at a very local level, and particularly among the UK's most vulnerable communities who are being routinely and cruelly targeted by organised criminal gangs.

As we increasingly live our lives online, we have found ourselves more and more at risk from cyber-enabled fraud. For the first time, this paper brings together experts from across the counter fraud community to highlight the scale of the threat and show how, by working more strategically together, we can help protect every one of us. The current coronavirus pandemic has caused many businesses to accelerate their digital strategies and move online more quickly than anticipated, and it has been alarming to see how quickly cyber fraudsters have responded to these changes and sought to take advantage of the global emergency for their own ends.

When I was asked to be part of this research in 2019, well before anyone knew anything about the coronavirus pandemic, I had no hesitation. Having worked in security for over 35 years, I know first-hand just how seriously British businesses take their responsibility to keep customers safe, and it is these businesses that are now at the frontline of combating cyber-enabled fraud. Recognising that fact, I have been keen to ensure that the voice of business is heard in the forthcoming National Cyber Security Strategy.

Criminals and, in some instances, state actors have used the power of the internet to industrialise fraud. This paper calls for a coherent response, better cooperation, sharing of intelligence and the need to support victims. Law enforcement, business and individuals must work more closely together to prevent harm and actively pursue and hold to account cyber criminals.

The near endemic nature of cyber fraud cannot be left unchecked with all the risks of damaging lives and undermining UK prosperity. This paper makes clear and assertive policy recommendations that will make a material difference to every one of us and the UK's reputation as a safe place to conduct business. ■

Executive Summary

THE UK PUBLIC is more likely to experience fraud than any other crime. Its widespread nature is partly because it is amplified by the internet, making it a cyber-enabled crime type. The scale of cyber fraud continues to increase at such a pace that it has become difficult to manage, let alone eradicate. It affects the UK public and businesses (both large and small) and undermines the functioning of a modern, digital society.

Despite its serious impact on the UK, cyber fraud has not received the appropriate level of coordinated response. Responsibilities for tackling the issue are unclear, creating a sizable leadership vacuum at the policy level. Financial institutions are usually the first line of defence in any instance of cyber fraud, and are often required to reimburse the victim. But to reduce the harm cyber fraud is having on society, there must be a reduction in the number of victims in the first instance. In the current model, this puts enormous pressure on UK law enforcement agencies and financial institutions to work together effectively. Pursuing criminals, reducing the crime rate and preventing re-victimisation remain key law enforcement responsibilities that require a functioning relationship between them.

Cyber fraud occurs over three main stages, prompting a multi-pronged response involving a range of stakeholders. First, data is unlawfully obtained from victims via various means including social engineering or phishing emails, leading to the theft of data from individuals or businesses. Next, stolen data is used to fraudulently transfer or divert funds into accounts controlled by criminals. Finally, the illicitly obtained funds must then be moved and laundered to conceal their origin. Despite wide variation in the type of victims and perpetrators involved (from individual opportunist criminals to sophisticated international organised crime groups), all stages of cyber fraud present pinch points for financial institutions and law enforcement agencies to detect and prevent the successful commission of the crime.

The aim of this paper is to provide targeted, long-term recommendations for stakeholders across government, law enforcement and the private sector by delineating roles and responsibilities for tackling cyber fraud. In doing so, the authors recommend that the existing components for tackling cyber fraud require an ambitious strategic approach to use current stakeholders and mechanisms effectively. The findings and conclusions are based on in-depth qualitative and quantitative research comprising a literature review, interviews, workshops and a survey, engaging with stakeholders from across these sectors.

The paper outlines several significant issues hampering the current model. Research has highlighted a worrying lack of clarity regarding the definition, understanding and measurement of cyber fraud (and of fraud more generally). There are differences in the way incidents are defined and recorded between financial institutions and law enforcement agencies, suggesting a need to standardise terminology and reporting practices.

The current model suffers from contrasting levels of prioritisation of cyber fraud across different stakeholders. Some financial institutions see cyber fraud as a high priority due to the risk of reputational damage, while others are more likely to think of it as just another cost of doing business. Meanwhile, for most law enforcement agencies, it is not always considered a high priority compared to violent or drug-related crimes due to its less visible and less physically harmful nature. The lack of sufficient funds for police to respond to cyber fraud cases effectively is another by-product of its seemingly victimless nature. Moreover, when operations are conducted successfully, their impact does not always receive sufficient visibility and recognition. This can make prioritising cyber fraud for law enforcement a thankless pursuit and therefore undesirable.

Information sharing between law enforcement agencies and financial institutions is inefficient and lacks buy-in. Despite numerous information-sharing partnerships and industry forums, significant limitations remain in the processes used to share information and in the quality of data that is provided. An effective system, proposed in this paper, would require sustainability, scalability, reciprocity and multi-functionality. None of the existing partnerships are assessed as fulfilling these four criteria.

Successfully prosecuting the perpetrators of cyber fraud remains a significant barrier due to the international nature of the crime and a reliance on cross-border alignment. The cost and time of investigations often compound this issue. Alternative models of pursuing criminals should be considered to help tackle cyber fraud. Law enforcement efforts should be built around a 'pursue' response that uses disruption activities like technical takedowns, while exploring practical avenues for arrests and asset recovery where possible. Underlying this should be a focus on protecting vulnerable people from becoming victims of cyber fraud, ensuring that they receive a service befitting of the harm caused by the crime.

As technology continues to develop, the cybercrime landscape is rapidly evolving, requiring an agile, coordinated and strategic approach across law enforcement, government and the private sector. To build an effective response to the threat, this paper calls on the Home Office to lay out the UK government's vision for tackling cyber fraud in a dedicated strategy underpinned with investment. This strategy should be designed and implemented with the support of UK business. The authors outline a series of recommendations which should form the basis of this approach moving forward.

Recommendations

THIS PAPER CALLS for a new UK cyber fraud strategy that is genuinely co-created with key stakeholders outside government. The central vision of the new cyber fraud strategy should be a greater role for financial services and wider private sector companies. While this paper does not call for radical changes to existing law enforcement structures, here are some actionable ways to deliver this primary recommendation:

Recommendation 1: The National Crime Agency and City of London Police should embark on upscaling 'pursue' activities to include a more prominent role for pre-emptive technical takedowns and private sector partnerships.

Recommendation 2: Prosecutions and arrests must remain a core part of the overall law enforcement approach to raise the risk and reduce the rewards of committing cyber fraud, but only where there is a realistic chance of securing convictions or recovering the proceeds of crime.

Recommendation 3: The National Police Chiefs' Council should work with the Home Office to implement a set of key performance indicators for cyber fraud policing. This will reflect the value of an effective 'protect' function for actual and potential victims, and a 'prevent' function focused on deterring potential criminals and reoffenders.

Recommendation 4: As the National Cyber Security Centre has done for cyber security, the National Economic Crime Centre should act as the central agency for 'protect' activities and publish clear advice for potential victims.

Recommendation 5: The National Crime Agency, in consultation with the Information Commissioners' Office, should publish comprehensive guidance for private sector organisations on how they can lawfully assist law enforcement in preventing and investigating cyber fraud through information sharing.

Recommendation 6: The National Economic Crime Centre should take primary responsibility for ensuring that at least one of the relevant information-sharing programmes satisfies four key criteria for effectively sharing information on cyber fraud threat actors:

1. **Permanence**. Operating on more than an ad-hoc basis.
2. **Scalability**. Encompassing a significant number of participants, which the Joint Money Laundering Intelligence Taskforce does not do.
3. **Two-way cooperation**. Allowing both private–public and public–private information sharing.
4. **Multi-functionality**. Being used for investigation purposes rather than only cyber security, which the Cyber Security Information Sharing Partnership does not allow.

Recommendation 7: The National Crime Agency, UK Finance, Cifas and City of London Police should bring partners together for a pilot initiative focused on more effective integration of cyber, anti-money laundering and fraud data, and disseminate sanitised examples of best practice.

Recommendation 8: Law enforcement agencies should consistently acknowledge the role of companies involved in cooperative takedowns of cybercriminal infrastructure.

Recommendation 9: Organised by the City of London Police and the National Economic Crime Centre, a large-scale national secondment programme for staff of financial institutions and cyber threat intelligence companies should be rolled out to equip police forces with improved skills in investigating cyber fraud.

Recommendation 10: The Economic Crime Academy should create a new Specialist Cyber Fraud Investigator course, which focuses specifically on the intersection between cyber and fraud investigations.

Recommendation 11: The Home Office should provide increased resourcing for the National Economic Crime Victim Care Unit to ensure that the service can reach a wider range of residents in more force areas.

Introduction

FRAUD HAS A significant impact on the UK economy, with one study estimating it to cost the UK economy an annual average of £190 billion.[1] The majority of fraud affecting the UK involves the internet,[2] and can therefore be referred to as 'cyber-enabled fraud' or, for brevity, simply 'cyber fraud'. This paper considers the roles and responsibilities of stakeholders in the ecosystem in reducing the levels of cyber fraud and instilling public confidence in the UK's response to it.[3]

The main difficulty in building a strong response to cyber fraud is the diversity of stakeholders involved and the lack of common direction in their activities. Government authorities, law enforcement agencies, financial institutions, private sector industry associations, and cyber security and technology companies all hold information relevant to the detection and investigation of cyber fraud but have no effective way of pooling it together.

Nor is there a central vision from the government as to what each of those categories of stakeholders is expected to do in order to contribute to a whole-of-system response to cyber fraud, let alone a framework that would create the incentives for them to do so.[4] This is despite the 2019 Conservative Party Manifesto committing to 'the creation of a new national cyber-crime

1. This estimate is taken from University of Portsmouth Centre for Counter Fraud Studies, 'Annual Fraud Indicator Report 2017', August 2017, p. 3. For details on the methodology used, see p. 9 of the report. Given that most fraud is highly underreported – including credit card, business and public sector fraud – this estimate is meant to serve as an indicator rather than an exact figure.
2. Exact figures on the amount of internet-related fraud in the UK vary. The Office of National Statistics' (ONS) Crime Survey for England and Wales 2018 put this number at 54%, while the former head of economic crime at City of London Police, Karen Baxter, stated in June 2020 that 86% of fraud now has some cyber-enabled aspect. See ONS, 'Crime in England and Wales: Year Ending December 2018', 25 April 2019; House of Commons, 'Home Affairs Committee: Oral Evidence: Home Office Preparedness for Covid-19 (Coronavirus)', HC 232, 3 June 2020; author interview with an information-sharing platform representative, 22 July 2020; Metropolitan Police, 'The Little Book of Big Scams', 5th edition, p. 5, <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/the-little-book-of-big-scams.pdf>, accessed 11 November 2020.
3. Please see Figure 3 for a detailed outline of this ecosystem. It broadly refers to law enforcement agencies, policymakers within UK government, financial services companies, regulators, cyber security companies, and industry associations and information-sharing partnerships.
4. Author interview with a policy professional at an information-sharing platform, 23 September 2020; author interview with a senior leader at an industry association, 11 September 2020; author interview with an information-sharing platform representative, 22 July 2020; author interview with a law enforcement officer, 22 July 2020; author interview with a law enforcement officer, 6 August 2020; author interview with a cyber security company representative, 16 July 2020; author interview with

force'.[5] With cyber fraud engaging various parts of the government's machinery, it is not clear which agency or minister has the overarching responsibility and oversight of all those individual parts. Similar to the UK government's approach to cyber security prior to the adoption of the 2016 National Cyber Security Strategy,[6] the model for tackling cyber fraud could be described as 'alphabet soup' and would benefit from stronger central direction.[7]

There is also the fragmentation of responses to various types of cyber fraud. The very notion of cyber fraud encompasses a broad array of crimes: from technically advanced to relatively unsophisticated; from the immensely profitable ones to those that hardly generate any money at all; from those perpetrated by wrongdoers within the UK to those that originate far beyond its borders. The overarching challenge for UK law enforcement agencies is to consistently prioritise those crimes that merit the most attention and ensure that the skills of the investigator match the profile of the crime – a task made more difficult due to the cyclical nature of priority setting in many law enforcement agencies. This is particularly complicated in the context of cyber fraud because what may appear to be a simple phishing email could contain sophisticated malware whose analysis – and therefore the investigation of the criminal actors behind it – would require specialist cyber forensic capabilities.[8]

In view of these challenges, this paper examines the current model for tackling cyber fraud and offers recommendations aimed at clarifying the roles of various stakeholders and bolstering their responses.

Methodology

This research stemmed from the desire to voice the concerns of business and law enforcement agencies ahead of the adoption of the next UK National Cyber Security Strategy. While cybercrime is a great concern for policymakers, cyber fraud in particular has proliferated at an alarming pace. Through this research, the authors seek to provide a reference point for a more ambitious, collective approach to tackling cyber fraud.

Data collection and analysis for this paper was guided by the central research question, 'what are the fundamental roles and responsibilities of different stakeholders in reducing the levels of

---

a financial investigator at a building society, 16 July 2020; author interview with a fraud technology specialist at a technology provider, 6 August 2020.

5. Conservative and Unionist Party Manifesto, 'Get Brexit Done: Unleash Britain's Potential', 2019, p. 9.
6. HM Government, 'National Cyber Security Strategy 2016–2021', 2016.
7. Jamie Collier, 'The UK's Alphabet Soup: The Organization of Cybersecurity Actors Protecting Critical National Infrastructure', Centre for Technology and Global Affairs, University of Oxford, 2019.
8. Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2020', 5 October 2020, p. 8. One type of phishing email is intended to dupe a target into falsely logging into a malicious domain with an attacker then retrieving their login details. A more technical intervention is a phishing email that delivers malware to a victim that penetrates the device's defences and transmits information to the attacker.

cyber fraud and instilling public confidence in the UK's response to it?'. The project adopted a mixed methods research design incorporating interviews, focus groups and a statistical survey. First, semi-structured interviews provided an in-depth understanding of the key short- and long-term challenges that organisations must prioritise. Workshops were then organised to bring these stakeholders together to exchange viewpoints and garner an appreciation of their priorities. A statistical survey allowed the views of a large number of respondents who could not be interviewed to be incorporated into the research process and provided findings with valuable quantitative data to supplement qualitative findings. Finally, members of the steering committee were drawn from all corners of this stakeholder community, providing constant reminders of what action is desirable and feasible among different stakeholder groups.

This paper is based on a mixed methods study comprising the following research methods:

- **Literature review**. The project began with a review of publicly available sources to identify the current stakeholder landscape and life cycle of cyber fraud. These sources included government policy documents, academic articles, court case materials (including indictments), reports by cyber security companies and other private sector organisations, and news reports. The literature review culminated in an interim briefing paper.[9]
- **Semi-structured interviews**. The research team conducted 37 semi-structured interviews with subject-matter experts from across UK law enforcement, government agencies, international organisations, academia and the private sector. A non-probabilistic, purposive sampling strategy was used to identify individuals with specific knowledge of the subject matter under examination. Other research participants were then identified by way of snowball sampling. The semi-structured interviews took place online between June and September 2020. Interviews were conducted on an anonymous basis to allow individuals to speak openly about potentially sensitive or contentious issues.
- **Two research workshops**. The research team conducted two online workshops in October 2020 to validate preliminary findings from the literature review and interviews. The stakeholder mix of organisations in the workshops was deliberately broad to gather valuable insights from conversations. The workshops were held digitally under the Chatham House Rule.[10]
- **Survey**. In the final stage of the project, a closed-ended statistical survey was distributed to a sample of UK law enforcement agency and financial services personnel. The survey

9. Sneha Dawda, Ardi Janjeva and Anton Moiseienko, 'Rethinking the UK Response to Cyber Fraud: Key Policy Challenges', RUSI Briefing Paper, July 2020. This paper outlines the challenges faced in responding to the threat from cyber-enabled fraud in the UK by looking at the life cycle of cyber fraud. It also provides an overview of the challenges in combating cyber fraud over the next decade and beyond.
10. 'When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed'. See Chatham House, 'Chatham House Rule', <https://www.chathamhouse.org/about-us/chatham-house-rule?gclid=EAIaIQobChMInuKm5ev67AIViKztCh20fwgzEAAYASAAEgLVDfD_BwE>, accessed 6 November 2020.

elicited 180 total responses. Of these, 66% (119) identified themselves as law enforcement representatives, 23% (42) as financial services personnel and 11% (19) as 'other', which included academic researchers, cyber security experts and intelligence analysts. The survey was distributed online via several bulk mailing lists managed by partner law enforcement agencies and financial institutions. The survey was first piloted with a small (convenience) sample of 11 respondents, and the questions updated accordingly to ensure clarity and accuracy. The survey results provide valuable quantitative findings to supplement the qualitative data gathered through interviews and focus groups.

- **Steering committee meetings**. To build in appropriate oversight of the research process, a steering committee was created that consisted of senior experts with expertise in cyber security, cybercrime, policing, banking and technology. Three steering committee meetings helped ensure the relevance, timeliness and robustness of the research.

Limitations

To the best of the authors' knowledge, this paper is the most up-to-date and complete attempt to answer the questions it set out to address. However, like any research paper, it has several limitations. External validity may be limited beyond the time period and locations in which the research was conducted and thus findings may only be representative of the UK context. It is also important to note the limitations inherent in the interview methods used – for instance, the research team did not interview representatives from all organisations in the ecosystem.

Regarding the survey, the target population comprised UK law enforcement and financial services personnel involved in fraud and cybercrime investigations. Due to the inherent difficulties in calculating the total size of this target population, it is impossible to statistically quantify the extent to which the sample size of 180 is representative of the wider population. For this reason, the results reported here should be interpreted as reflecting the views of the 180 individuals sampled; external generalisability should not be assumed.

Structure

To answer the research question, Chapter I outlines the modern nature of the cyber fraud threat to make clear what it is that stakeholders must address. It defines what cyber fraud is, analyses the threat it poses during the ongoing coronavirus pandemic and explores the nature of cyber fraud victimisation. Chapter II discusses the current state of the response to cyber fraud in the UK by mapping out the relevant stakeholders and where they stand in relation to each other. Finally, Chapter III identifies possible improvements to the current model of tackling cyber fraud that can be implemented by public and private sector actors.

I. Cyber Fraud in the UK

CYBER FRAUD IN the UK is rampant, costing millions of pounds and leaving victims in its wake. This research is not only relevant in tackling the problem, but also timely. The UK's next National Cyber Security Strategy is expected in 2021 and will revise the government's approach to cyber security. This may include policies around cyber security as an enabler of economic security by safeguarding users, networks and systems. Related to this, economic security and prosperity have been significantly undermined due to the coronavirus pandemic, creating a pressure to safeguard what current wealth people possess. This paper seeks to build a blueprint for a safer, prosperous and digitally driven UK.

The UK's response to cyber fraud is partly dependent on: how the term is understood; who is believed to be involved in perpetrating it; what the severity of the threat is thought to be; and who the victims are. This chapter addresses each of these issues.

Defining and Measuring Cyber Fraud

> 'Cyber-enabled fraud is fraud. Let's talk in language that consumers understand'.
> – Interview participant from an information-sharing platform, 22 July 2020.

How different stakeholders understand the term 'cyber fraud' can determine their approach to tackling it. In UK law enforcement agencies, different teams normally assume responsibility for investigating cyber-enabled and cyber-dependent crime respectively.[11] Those decisions include who is involved, how they share information and who is in charge. This can be problematic because cyber fraud often flows from a data breach because of, for instance, malware infection, necessitating the involvement of a more specialist 'cyber' skillset which may be housed in a separate team or department.[12]

---

11. Second workshop, 9 October 2020. Cyber-dependent crimes are defined by the Crown Prosecution Service (CPS) as 'crimes that can be committed only through the use of Information and Communications Technology ("ICT") devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity)'. The CPS defines cyber-enabled crimes as 'traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft)'. See CPS, 'Cybercrime – Prosecution Guidance', updated 26 September 2019, <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>, accessed 6 November 2020.
12. Author interview with a law enforcement professional at a regional organised crime unit (ROCU), 12 August 2020.

That said, the practicality and utility of the term 'cyber fraud' is sometimes contested.[13] It can cover types of fraud that differ dramatically in the level of technological sophistication involved.[14] Action Fraud, the UK's primary fraud and cybercrime reporting organisation, has multiple different categories of frauds under the term 'cyber fraud' in its glossary.[15] To complicate the definition further, the majority of fraud now has an online component. A standardisation of terms would therefore be helpful. For instance, Europol created a taxonomy of terms to use for the national network of Computer Security Incident Response Teams (CSIRTs) to ensure they were aligned.[16]

For the purposes of this project, 'cyber fraud' refers to financially motivated cybercrime which results in fraud. This includes attacks that specifically use data exploitation, stolen or bought, to commit fraud. These cyber frauds that rely on the theft or use of stolen data require a response based more on technical security solutions to prevent data theft by criminal actors. Where we refer to 'digitally enabled frauds', such as romance and investment frauds, they demand a more victim-centric, behaviourally driven response focused on avoiding risky interactions online. Despite the differences between cyber fraud and digitally enabled fraud, there are commonalities. For example, both types of fraud are high in volume, have a strong international component and a digital footprint. Despite the focus on cyber fraud, the analysis in this paper is relevant to overcoming barriers across both definitions.

There is similar uncertainty around the metrics used to measure cyber fraud. Current public metrics are vague and do not encompass both cyber and fraud components of the crime. For instance, monetary estimates of harm alone may prove to be a superficial indicator for the public that does not tangibly advance efforts to tackle cyber fraud, but rather seeks to shock.[17] Instead, victim profiles, trends and analysis of the threat are likely to aid law enforcement agencies and

13. Author interview with a law enforcement officer, 10 September 2020; author interview with a law enforcement officer, 29 July 2020; author interview with a law enforcement professional at a ROCU, 29 July 2020.
14. Author interview with a fraud specialist at an industry association, 10 September 2020.
15. Action Fraud is managed by the City of London Police and is the primary tool for fraud reporting in the UK. Any victim of fraud is encouraged to report to Action Fraud – they are assigned a crime number and their case, if deemed investigable, is triaged to the relevant law enforcement agency. The fraud types listed under the category 'cyber fraud' on Action Fraud's website are: bot-net-related fraud; facility takeover; fraud-enabling activities; phishing; proxy servers; click fraud; computer hacking; computer software frauds; internet dialler scam; invoice scams; tabnapping; domain name scams; malware and computer viruses; and website domain name scams. See Action Fraud, 'A-Z Fraud', <https://www.actionfraud.police.uk/a-z-of-fraud-category/cyber-fraud>, accessed 6 November 2020.
16. Europol, 'Cyber Intelligence', <https://www.europol.europa.eu/activities-services/services-support/intelligence-analysis/cyber-intelligence>, accessed 6 November 2020.
17. While 'shock' may be seen as superficial, it can be useful in raising public support or attention to an issue. Author interview with an ex-law enforcement officer at a non-governmental organisation, 5 August 2020.

financial institutions in their strategic response.[18] The National Fraud Intelligence Bureau (NFIB) within the City of London Police has a live dashboard of fraud statistics and reporting.[19] It breaks down the fraud types and provides statistics on victim profiles and local forces. One area the dashboard may build on is in reflecting the amount of fraud involved in different methods of intrusion such as phishing. Another is to create a third tab to filter for cyber fraud, appropriately acknowledging the linkages between cybercrime and fraud.

Life Cycle of Cyber Fraud

To assess possible interventions against cyber fraud, it is helpful to understand its life cycle, or the process involved in its commission. What is a single fraud from the victim's perspective may involve acts committed by individuals who buy and sell personal data, those with the technical capability to launch a cyber attack and those who specialise in recruiting 'money mules' to cash out the proceeds of crime, as summarised in Table 1.

18. Author interview with a retired law enforcement officer at a non-governmental organisation, 5 August 2020.
19. City of London Police, National Fraud Intelligence Bureau, 'NFIB Fraud and Cyber Crime Dashboard', <https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/6049930456504 5b0bce05d2ca7e1e56c>, accessed 6 November 2020.

Table 1: The Life Cycle of Cyber Fraud

Stages	Process
Cyber attacks and data theft	Most fraud cases affecting the UK involve the use of the internet to unlawfully obtain victims' personal information, such as names, dates of birth, bank details and National Insurance numbers.* Social engineering is one of the primary mechanisms for eliciting this information.† Phishing is one of the most prevalent forms of social engineering, with fraudsters circulating malicious links or files under the guise of a legitimate email. Increasingly, personal identifiers can be found and triangulated via open source means: social networking, dating and employment sites are all valuable sources of information for criminal groups. The more of this information that can be collated, the more tailored an attack can be to a particular individual, and the higher the risk of being vulnerable to repeat victimisation in the future. At the business level, areas of risk include company accounts, client databases and intellectual property. Business email compromise is one of the most important threats for businesses, particularly those with less cyber hygiene awareness.‡ The 2020 Cyber Breaches Survey found that, potentially, the 'fraud aspect of phishing attacks, rather than the risks from malicious code … are being considered more disruptive to work flows' for businesses.§ The impact of a breach is particularly significant for a business's reputation, profit and reliability of service.

Stages	Process
Using stolen data to commit fraud	The next stage in the cyber fraud life cycle is using stolen data to commit fraud. In some cases, an organised crime group will carry out the fraud themselves, convincing their target of the legitimacy of their interaction – perhaps over several days, weeks or months – and diverting money into accounts controlled by the criminals. Alternatively, the data that has been harvested may be sold on criminal marketplaces on the dark web.‖ Cryptocurrencies, especially Bitcoin, are often used to purchase datasets containing credentials and passwords.¶ While companies in financial services are prominent targets for dark web trading,** individuals are also at risk given the size of their digital footprint relative to their capacity to protect themselves. It has been suggested that the average person suffers eight unlawful disclosures of their data in their lifetime.††
Money laundering of the proceeds of cybercrime	Funds obtained via the means described above must be moved and spent by criminals. These will usually be channelled through multiple bank accounts in the UK to obfuscate the money trail before the money is sent on to an overseas jurisdiction. Individual money mules are often recruited but corporate accounts are also used for larger payments to avoid triggering immediate suspicion that would lead to the freezing of the account. Funds in fiat currency can also be converted into cryptocurrency to further obfuscate the money trail and move value across borders. In that case, the funds in cryptocurrency would ordinarily have to be exchanged back into fiat currency given the limited mainstream adoption of cryptocurrency.

*Sources: * Sneha Dawda, Ardi Janjeva and Anton Moiseienko, 'Rethinking the UK Response to Cyber Fraud: Key Policy Challenges', RUSI Briefing Paper, July 2020; † Social engineering is a 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?', 26 August 2020, <https://www.kaspersky.co.uk/resource-center/definitions/what-is-social-engineering#:~:text=Social%20engineering%20is%20a%20manipulation,giving%20access%20to%20restricted%20systems>, accessed 6 November 2020; ‡ National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime 2020', p. 48; § Department for Digital, Culture, Media and Sport, 'Cyber Security Breaches Survey 2020', updated 26 March 2020, <https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020#chapter-5-incidence-and-impact-of-breaches-or-attacks>, accessed 6 November 2020; ‖ 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 6 November 2020; ¶ 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 6 November 2020; ** F-Secure, 'Cyber Threat Landscape for the Finance Sector', July 2019; †† Emma Dunkley, 'UK: Scammers Bouncing Banks into Sham Loans', KYC 360, 5 October 2020, <https://www.riskscreen.com/kyc360/news/uk-scammers-bouncing-banks-into-sham-loans/>, accessed 6 November 2020.*

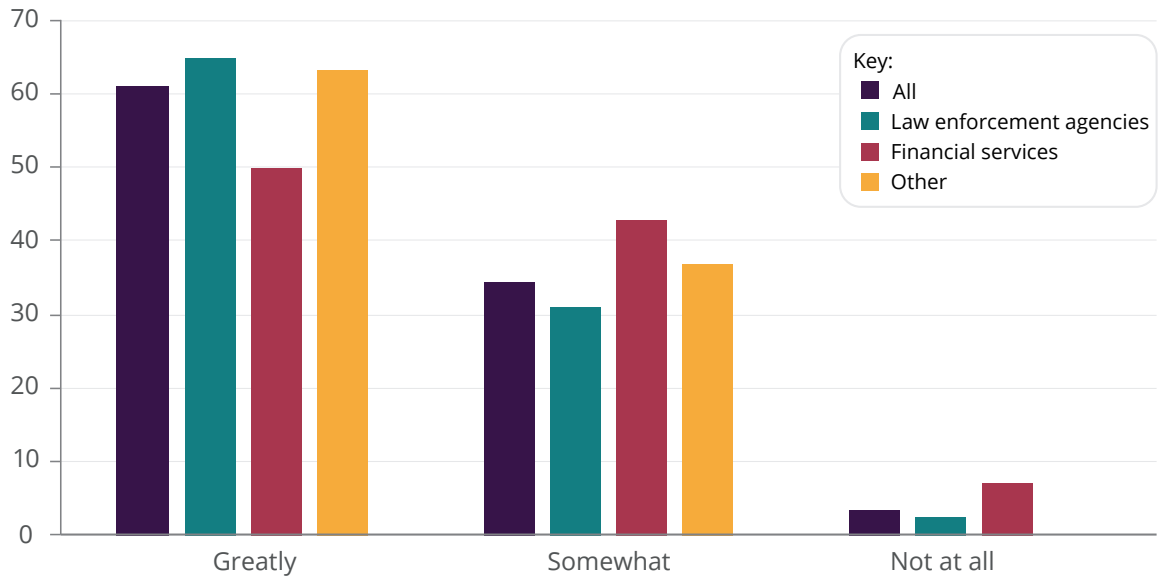
Note: The 'life cycle' model of cyber fraud was used in Dawda, Janjeva and Moiseienko, 'Rethinking the UK Response to Cyber Fraud', and Table 1 largely follows the same pattern outlined in that publication.

Cyber Fraud During the Pandemic

The coronavirus pandemic has undoubtedly had an impact on the cyber fraud threat landscape, although the extent of this remains unclear.[20] Organised crime groups (OCGs) were quick to take advantage of the situation, and the rapid digitalisation of both large and small businesses due to remote working has given rise to new vulnerabilities. As shown in Figure 1 below, a clear majority of survey respondents believe that the coronavirus pandemic has increased citizens' vulnerability to cyber fraud. While 61% believe it has 'greatly' increased, 34% believe it has 'somewhat increased'.

20. Second workshop, 29 October 2020.

Figure 1: In your view, to what extent has the coronavirus pandemic increased citizens' vulnerability to cyber-enabled fraud?



Source: Survey data.

Although the long-term impact of the pandemic is a significant 'unknown', some observations on the current threat landscape are offered below.

Threats to the State from Organised Crime Groups

Cyber fraud is perpetrated by a wide range of offenders from opportunist criminals to sophisticated OCGs. However, the scale at which OCGs have mobilised to systematically target public sector operations merits closer attention. In the UK, as in many other countries, the government rushed to ensure that individuals and businesses had access to finance that would allow them to survive the pandemic.[21]

With these measures, there inevitably came a significant risk of fraud. This is best exemplified by the Bounce Back Loan Scheme (BBLS), which came as a response to complaints that the Coronavirus Business Interruption Loan Scheme (CBILS) was moving too slowly, with onerous credit checks risking many legitimate businesses not getting the help they needed. More than

21. Such schemes included: the Coronavirus Job Retention Scheme; Coronavirus Business Interruption Loan Scheme; Bounce Back Loan Scheme; Self-Employment Income Support Scheme; and other measures like the deferral of VAT payments.

69,000 BBLSs costing over £2 billion were approved in the first day of the scheme's existence.[22] It has been claimed that the BBLS is one of the schemes most susceptible to fraud in the UK, with losses expected to exceed the 0.5% to 5% estimates for most public sector schemes.[23]

The methods that organised criminals have used will be familiar from the life cycle of cyber fraud discussed above. Personal data, including dates of birth and addresses, is obtained via phishing emails or website hacking, and may subsequently be traded on the dark web.[24] These details will be collated to create false applications for BBLS loans of up to £50,000, for example by setting up companies using a stolen identity and opening a business account.[25] Even though only companies established before March 2020 were able to apply, firms established as late as June 2020 have been used to take out loans.[26] It is worth noting that the UK law enforcement response to this heightened threat has not remained static. For example, the 'COVID-19 Fusion Cell' hosted at the National Economic Crime Centre (NECC), comprising over 30 organisations across the public and private sector, has allowed for more real-time financial intelligence sharing.[27] Lessons learned from this period must be captured and fed into longer-term preparations for public–private sector coordination.

Cyber Security Vulnerabilities

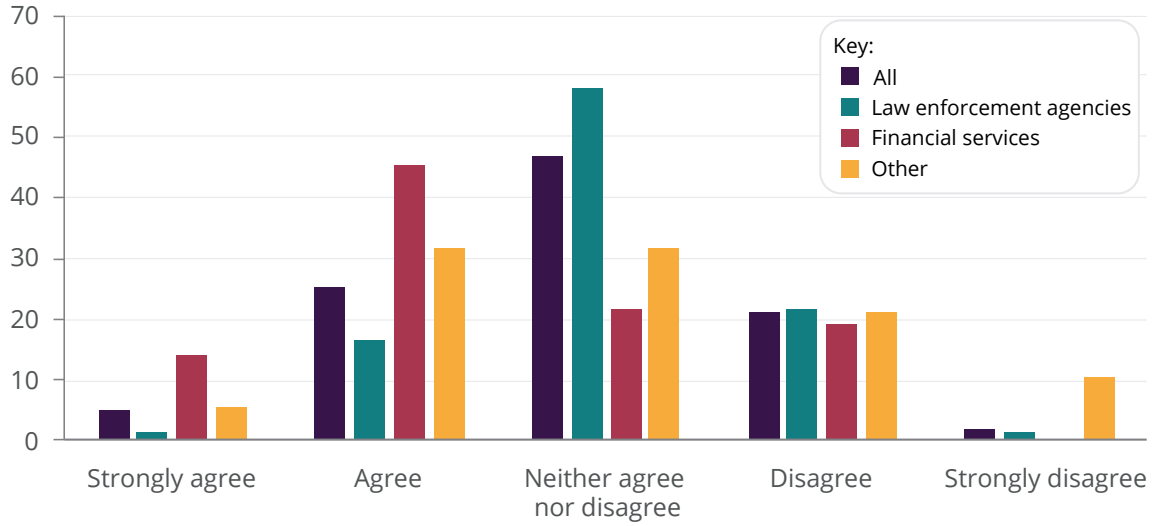
Managing the risks of remote working requires a strong grasp of the existing and future device management of employees, providing sufficient risk management tools. Onboarding new technology at a rapid rate also creates vulnerabilities for businesses, as evident from concerns around video conferencing security.[28]

It is concerning that the majority of the survey respondents for this research (70%) felt that the increase in remote working has not been matched by increased efforts from businesses to

22. HM Treasury, 'Over 69,000 Loans Approved in the First Day of the Bounce Back Loan Scheme', 6 May 2020.
23. Policy Exchange, 'Daylight Robbery: Uncovering the True Cost of Public Sector Fraud in the Age of COVID-19', 2020, p. 34; Chris Giles, 'HMRC Chief Warns Job Retention Scheme a Target for Organised Crime', *Financial Times*, 8 April 2020. See also Jasper Jolly, 'Organised Crime in UK Exploiting Coronavirus Loan Scheme', *The Guardian*, 2 October 2020.
24. Emma Dunkley, 'UK: Scammers Bouncing Banks into Sham Loans', 5 October 2020, <https://www.riskscreen.com/kyc360/news/uk-scammers-bouncing-banks-into-sham-loans/>, KYC 360, accessed 6 November 2020.
25. *BBC News*, 'Coronavirus: "My Name Was Used to Steal a Government Covid Loan"', 28 September 2020.
26. *Ibid.*
27. Koos Couvee, 'UK "Fusion Cell" Deploys Financial Intelligence Against COVID-19 Crime Wave', ACAMS Money Laundering, 5 November 2020, <https://www.moneylaundering.com/news/uk-fusion-cell-deploys-financial-intelligence-against-covid-19-crime-wave/>, accessed 25 November 2020.
28. Zoom was particularly affected by organisations' security concerns. See Ravie Lakshmanan, 'Researcher Demonstrates Several Zoom Vulnerabilities at DEF CON 28', *Hacker News*, 10 August 2020, <https://thehackernews.com/2020/08/zoom-software-vulnerabilities.html>, accessed 6 November 2020.

improve their cyber security and anti-fraud protection. On this, there was a clear difference in views between law enforcement agency respondents and financial institution respondents: 60% of the latter believe that the increase in remote working has been matched by increased efforts to improve protection, compared with just 18.5% of the former. A chi-square test[29] of independence showed that this difference was statistically significant.[30]

Figure 2: To what extent do you agree with the following statement? 'As remote working has increased, businesses have increased their efforts to improve cyber security and anti-fraud protection'



Source: Survey data.

It is important to recognise that there are concrete steps that can be taken to mitigate risk, such as managing the technology stack and ensuring devices are managed securely.

Vulnerabilities inherent in the home working environment are more difficult to address. Domestic wi-fi networks, for example, are commonly far less secure than business-operated networks.[31] There are numerous domestic devices connected at any one time, used by different people in the household with various levels of cyber awareness. KPMG aptly calls this the 'hostile home environment' because of poor endpoint management in place from domestic

29. A chi-square test is used to determine whether given variables are independent from each other or whether they are related.
30. X^2 (1, N = 161) = 25.29, p = <0.01.
31. Martin Roesler, 'Working From Home? Here's What You Need for a Secure Setup', Trend Micro, 26 March 2020, <https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup>, accessed 6 November 2020.

internet use, making the home network more vulnerable to attack.[32] It is difficult for a business to control the level of risk at this stage.

Due to the hostile home environment, employees must be equipped with adequate cyber awareness to keep themselves safe while using business and home devices. However, cyber security knowledge is often concentrated in a select few individuals in a company, typically in the IT department. Great amounts of trust are put on these individuals to maintain the security of their business devices, as they would do in an office environment. As a result, people often exhibit blind faith in the safety of the systems they use.[33] This presents an opportunity that criminals may seek to exploit and therefore requires significant upskilling of employees.[34]

For businesses, investing in their cyber security is vital. For small to medium enterprises, low-cost and simple certifications such as Cyber Essentials are attractive because they do not require extensive technical knowledge to implement.[35] There are further risk management options for smaller businesses. These include tools such as cyber insurance to prevent business interruption when required.

The Nature of Victimisation

There is a risk of overlooking the nature of victimisation and who suffers because of an inadequate societal response to cyber fraud. There are four main victim categories for cyber fraud: individuals who have been defrauded; the private sector (either directly or when bearing the financial cost of a customer fraud); the public sector (as in the bounce back loans described above); and society as a whole.

These categories are not mutually exclusive. A fraud can be committed against an individual which the bank later underwrites, and which – if repeated enough times – can affect a large enough proportion of people to be damaging to society as a whole. In each of these cases, the starting point is the individual experience. This is not only because of the scale and volume of frauds against individuals, but also the way these are increasingly being conducted. A report published in 2020 by the University of Portsmouth classified six key areas other than financial impact where victims are affected including: disruption (in terms of losing access to services and

32. Endpoint management – namely device management – is difficult in a home environment because of other domestic devices in the household with unpredictable levels of security. This can lead to compromise of the router. See KPMG, 'Key Cyber Risks for Banks During COVID-19', <https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html>, accessed 21 October 2020.
33. Gillian Tett, 'Why Covid-19 is a Gift for Cybercriminals', *Financial Times*, 15 July 2020.
34. Author interview with a financial investigator at a building society, 16 July 2020.
35. NCSC, 'About Cyber Essentials', <https://www.ncsc.gov.uk/cyberessentials/overview>, accessed 6 November 2020.

time spent responding to the incident); psychological and emotional impacts; health impacts; damage to reputation; violation of the digital self; and loss of digital possessions.[36]

That being said, the monetary loss that many victims experience can be overpowering, and it is not a foregone conclusion that victims will get a refund from their bank, particularly when 'effective warnings' are displayed at the point of payment.[37] Nor is it the case that victims' credit ratings are unaffected; these can take many years to recover if applications under their name have been made to multiple providers.[38] Whereas 'unauthorised' payment frauds tend to be seen as a banking problem, thereby absolving the victim of culpability, the increasing trend towards manipulative social engineering means that in many cases victims approve transactions they believe to be legitimate. These types of frauds are described as 'authorised push payment frauds',[39] and the data over the past five years shows a rapid growth, with a 29% increase in 2019 costing customers £456 million.[40]

Digitally enabled frauds, such as romance[41] or investment frauds,[42] lend themselves more to the targeting of individuals over businesses (although, in the business context too, 'verifying the legitimacy of a dubious email is harder when you are not sitting next to colleagues').[43] With that caveat in mind, the theme of fraudsters moving away from targeting businesses at an industrial

36. Mark Button et al., 'Victims of Computer Misuse: Main Findings', University of Portsmouth, April 2020. For an interpretation of organisational cyber harms, see Ioannis Agrafiotis et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity* (Vol. 4, No. 1, 2018), p. 8.
37. The Contingent Reimbursement Model Code is a voluntary initiative where banks reimburse faultless fraud victims. It states that fraud warnings must be 'understandable, clear, impactful, timely and specific'. Some banks tailor their fraud warnings to the associated risk of a specific type of payment (such as to a friend or business) and other banks offer a more generic message about bank transfer fraud. See Chiara Cavaglieri, 'Banks Denying Refunds to Scam Victims Who Ignore New Warnings', Which?, 24 January 2020, <https://www.which.co.uk/news/2020/01/banks-denying-refunds-to-scam-victims-who-ignore-new-warnings/>, accessed 6 November 2020.
38. Author interview with a policy official at an information-sharing platform, 22 July 2020.
39. In an authorised push payment fraud, the genuine customer is tricked, often using sophisticated social engineering techniques, into making the payment to another account which is controlled by a criminal.
40. UK Finance, 'Fraud – The Facts 2020: The Definitive Overview of Payment Industry Fraud', March 2020, p. 5.
41. Romance frauds happen when someone is tricked into thinking they have met a potential partner through an online dating site or social media network, but the person is operating a fake profile to gain their victim's trust and ultimately ask for money or a sufficient amount of personal information to steal an identity.
42. Investment frauds happen when a person receives a usually unsolicited call from someone offering the opportunity to invest in schemes or products whose value is grossly overstated or are completely non-existent. Most investment frauds are operated from offices known as 'boiler rooms'.
43. First workshop, 27 October 2020.

scale towards targeting individuals was reinforced in interviews and workshops conducted as part of this research. For all the protections that can be put in place to help individuals stay safe online, a bank cannot always increase a customer's level of protection directly, and a level of awareness and action is incumbent on customers themselves.[44] This leaves gaps which criminals can exploit, with some research participants conceptualising this as 'silent stealing':

> There's a working hypothesis that criminals are going down market. Yes, trying to steal £10 million from a bank is an option, but stealing £10 a hundred thousand times is going to give you a good return and probably go below the radar. Are you going to call Action Fraud or your bank in the case where you lose £10?[45]

In summary, although there is little doubt that cyber fraud poses a significant threat to the UK's prosperity, developing an effective response is complicated by the fact that 'cyber fraud' has many guises. It is an umbrella term that can cover different crimes, perpetrators and victims. However, as this chapter demonstrates, there are also common features that justify treating cyber fraud as a distinct law enforcement challenge. They include frequent reliance by criminals on the same basic steps of: obtaining stolen data, using it and cashing out the proceeds; rapid exploitation of emerging cyber security vulnerabilities, such as those resulting from the shift to online/home working during the coronavirus pandemic; and the potentially significant impacts on individual victims even if their economic losses are reimbursed. There are therefore several areas that UK stakeholders can focus on to increase the country's collective resilience to cyber fraud, and the following chapter examines the current state of this response.

44. *Ibid.*
45. *Ibid.*

II. Responses to Cyber Fraud in the UK

TACKLING CYBER FRAUD involves multiple stakeholders with various responsibilities, capabilities and incentives. This chapter discusses the contribution of: law enforcement agencies, which are responsible for investigating cyber fraud and providing victim care; financial institutions, which are both a key target for fraud and a means for moving the proceeds; cyber security and technology companies, which hold intelligence and possess technical resources that can help investigate cyber fraud and even carry out technical takedowns of cybercriminal infrastructure; and information-sharing arrangements, which bring together for a common purpose the information and intelligence that would otherwise be confined to a single organisation.

Research for this paper has highlighted a lack of sufficient oversight and coordination from central government to ensure a more coherent approach across the various stakeholders listed in Figure 3 is adopted.

Figure 3: The Stakeholders Involved in Tackling Cyber Fraud

Source: Author generated. A previous version of this map is presented in Sneha Dawda, Ardi Janjeva and Anton Moiseienko, 'Rethinking the UK Response to Cyber Fraud: Key Policy Challenges', RUSI Briefing Paper, July 2020. Research conducted for this paper warranted an update of that map.

Law Enforcement Agencies

Law enforcement agencies with a significant role in the cyber fraud response in England and Wales[46] are summarised in Table 2 below.

Table 2: Law Enforcement Agencies with Cyber Fraud-Related Responsibilities in the UK

Organisation	Role
City of London Police	The Commissioner of City of London Police is the NPCC Lead for Economic and Cyber Crime. City of London Police is also the National Lead Force for Fraud.* In this role, they have several priorities which different units within the force are responsible for delivering on: • Improve knowledge of serious organised fraud and allocate resources to high-harm threats. A key part of building this knowledge base is the reporting function carried out by Action Fraud and the review and dissemination function carried out by the National Fraud Intelligence Bureau alongside it. • Coordinate closely with the private sector, the National Economic Crime Centre (NECC) and wider policing to build capability and shared understanding across the counter-fraud community.† • Target criminal finances and conduct investigations for serious and complex fraud cases which local police forces do not have the capacity to take on. • Deter people from engaging in fraud and cybercrime. • The National Economic Crime Victim Care Unit (NECVCU) provides support for victims deemed to be especially vulnerable after a fraud or cybercrime, with the aim of reducing the chances of repeat victimisation.‡ Since being established, the NECVCU has helped over 70,000 people, with only six reporting another victimisation.§
National Crime Agency	The NCA has an important role in pursuing serious and organised fraudsters and, where possible, ensuring that the proceeds of crime are returned to victims. The NCA's UK Financial Intelligence Unit (UKFIU) is responsible for recording suspicious activity reports (SARs) and analysing them to extract strategic and tactical intelligence. They also have a role helping individuals and businesses develop resilience to cyber fraud. The National Cyber Crime Unit (NCCU) within the NCA aims to provide a joined-up national response to cybercrime. It has a role in investigating the most serious incidents of cybercrime, tasking cybercrime cases nationally, pursuing criminals nationally and internationally, and working proactively to exploit criminal vulnerabilities and disrupt attacks before they happen.‖

46. The research team's analysis of the law enforcement framework is limited to England and Wales, but the findings based on this analysis are likely to apply to the UK as a whole.

Organisation	Role
National Economic Crime Centre (NECC)	The NECC was established in 2018 to act as a central point of coordination for the UK's response to economic crime. It brings together public and private sector intelligence and capabilities to prioritise areas of investigation and share best practice.[¶] The NECC coordinates the activities of the Joint Money Laundering Taskforce (JMLIT), a public–private partnership that includes over 40 financial institutions and involves the exchange of both operational information and typologies.[**] The NECC also publishes public–private threat updates that identify key areas of concern.
National Cyber Security Centre (NCSC)	The NCSC is part of GCHQ and was formally established in 2017. It is the UK's national technical authority and defence against cyber attacks. The NCSC houses the UK Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT), defending critical national infrastructure, supporting industries and businesses in their cyber resilience, and disseminating advice to individuals. The NCSC also runs the Active Cyber Defence (ACD) programme which manages eight tools to protect public sector networks and users.[††] These are technical interventions run with private sector organisations such as Nominet. One such tool is the NCSC Suspicious Email Reporting Service (SERS), developed in partnership with City of London Police, which encourages individuals and businesses to forward details of suspected phishing emails. The most recent figures state that 2,930,000 reports have been made, with the removal of 13,291 scams and 30,344 URLs.[‡‡] Additionally, the NCSC is involved in an initiative called 'Project FORTIS', which intends to simplify and enhance the cyber incident reporting experience for victims and those responding to incidents.[§§]
Regional Organised Crime Units (ROCUs)	ROCUs provide local police forces with access to a standardised set of capabilities to aid their efforts against serious and organised crime.[‖‖] There are 10 ROCUs across England and Wales, and although each is meant to have a minimum standard across all 13 specialist capability areas (which include cybercrime investigation and fraud), they differ from each other in size and resourcing. ROCUs are an important bridge between the NCA and local police forces, and regularly work with SMEs and charities in response to specific threats. Their in-house capabilities, alongside their link into the NCSC, enables them to provide support in the event of a cyber incident, irrespective of whether a formal police investigation exists.[¶¶] ROCUs also include Regional Economic Crime Units and Regional Cyber Crime Units, which are engaged in the response to cyber fraud too.

Organisation	Role
Local police forces	Local police forces have the responsibility to act on the crime and intelligence referrals they receive from the NFIB and partner agencies by conducting investigations and providing support for victims in their local area. Once the investigation is complete, they will pass on the case to the Crown Prosecution Service (CPS) who are then responsible for securing a judicial outcome for cases.
National Police Chiefs' Council (NPCC)	The NPCC acts as a central coordinating body for police forces in the UK to coordinate operations, help set requirements and priorities,[***] evaluate performance and share best practice.[†††] The NPCC has also dedicated a Fraud and Cyber Lead portfolio to the Commissioner of City of London Police[‡‡‡] with the aim of facilitating further integration of fraud and cyber policing activities.
Police and Crime Commissioners (PCCs)	PCCs are elected by the public to hold their local police forces to account. Their role is to ensure community needs are met effectively and improve relationships both with the public and with a range of agencies across the country to facilitate a unified response to crime. PCCs set the police and crime objectives for their area through a police and crime plan. In these plans, there is often variation in the extent to which fraud and cyber are prioritised across the country. They also have a role in making sure that asset recovery and the proceeds of crime are redistributed towards the economic crime response.
International law enforcement	UK law enforcement agencies frequently need to coordinate with agencies outside of the UK, although there are jurisdictions which are notoriously hard to enlist during an investigation. Examples of key partners include Europol, Interpol, the FBI and EU member states' national police forces.

Sources: [*] Home Office, 'Transparency Data: National Lead Force for Fraud', updated 9 December 2020, <https://www.gov.uk/government/publications/national-lead-force-for-fraud/national-lead-force-for-fraud>, accessed 4 January 2021; [†] See, for instance, City of London Police's Cyber Griffin project, <https://cybergriffin.police.uk/>, accessed 29 January 2021; [‡] Action Fraud, 'National Economic Crime Victim Care Unit (NECVCU)', <https://www.actionfraud.police.uk/economic-crime-victim-care-unit-ecvcu>, accessed 6 November 2020; [§] Author interview with law enforcement officer, 29 July 2020; [‖] NCA, 'National Cyber Crime Unit', <https://web.archive.org/web/20131014171419/http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit>, accessed 6 November 2020; [¶] NCA, 'National Economic Crime Centre', <https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed 6 November 2020; [**] Ibid; [††] NCSC, 'Active Cyber Defence (ACD)', <https://www.ncsc.gov.uk/section/products-services/active-cyber-defence>, accessed 6 November 2020; [‡‡] NCSC, 'Phishing: How to Report to the NCSC', <https://www.ncsc.gov.uk/information/report-suspicious-emails>, accessed 6 November 2020; [§§] Paul Morgan-Bentley, 'Spies to Run Cybercrime Hotline After Scandal at Action Fraud', The Times*, 5 February 2020; [‖‖] HMIC, 'Regional Organised Crime Units: A Review of Capability and Effectiveness', November 2015, <https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/regional-organised-crime-units.pdf>, accessed 6 November 2020; [¶¶] NCSC, 'Regional Organised Crime Units (ROCUs)', <https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus>, accessed 6 November 2020; [***] See, for example, Home Office, 'The Strategic Policing Requirement', March 2015; [†††] See, for example, NPCC, 'Specialist Capabilities', <https://www.npcc.police.uk/NPCCBusinessAreas/ReformandTransformation/Specialistcapabilitiesmain/SpecialistCapabilities.aspx>, accessed 6 November 2020; [‡‡‡] First workshop, 27 October 2020.*

Financial Institutions

In the context of cyber fraud, financial institutions play a triple role in that they may:

1. Fall victim to a cyber attack that may result in a leak of personal data or funds held by the institution.
2. Be asked by the victim customer to process a payment for the fraudster's benefit.
3. Be involved in the movement or spending of the proceeds of cyber fraud.

In each of these scenarios, different sets of obligations and risks come into play, as summarised in Table 3.

Table 3: Financial Institutions' Obligations and Risks in Relation to Cyber Security Breaches, Fraudulent Payments and Money Laundering

Data Breach	Fraudulent Payment	Money Laundering
Obligations		
If a data breach occurs and it is likely to have an adverse impact on individuals' rights or freedoms, any organisation that suffers such a breach (not only a financial institution) must notify the Information Commissioner's Office.* If the fraud is significant by reference to its size, reputational impact or because it reflects a weakness in internal controls, a regulated firm must report it to the FCA.†	If a victim asks the financial institution to process a payment, **banks will in many cases reimburse the victim** based on the Contingent Reimbursement Model Code for Authorised Push Payment Scams (CRM Code), a voluntary initiative which a number of banks signed up to in May 2019.‡ The CRM Code covers situations where the customer 'transferred funds to another person for what they believed were legitimate purposes but which were in fact fraudulent'. Financial institutions will also reimburse individuals in cases of unauthorised fraud.	Regulatory obligations under the Money Laundering Regulations 2017§ and criminal offences contained in the Proceeds of Crime Act 2002 are aimed at preventing financial institutions from facilitating money laundering. These include obligations related to **customer due diligence** and **suspicious activity reporting**.
Risks		
Cyber security breaches pose financial, reputational and regulatory risks. Customer payment data is a frequent target for criminals. This can lead to serious business interruption and remediation costs.	Fraud is often seen as a **cost of business** that the institution is prepared to bear within certain limits.‖	Money laundering does not directly harm the financial institution but can lead to significant **regulatory penalties** if it reflects a weakness in the institution's control.

*Sources: * Information Commissioner's Office, 'Personal Data Breaches', <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#ib2>, accessed 20 October 2020; † FCA, 'Fraud, Errors and Other Regularities', FCA Handbook, SUP 15.3.17; ‡ Lending*

Standards Board, 'Contingent Reimbursement Model Code for Authorised Push Payment Scams', May 2019, <https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/>, accessed 20 October 2020; § Binding on certain regulated sectors, including but not limited to financial institutions; ‖ Author interview with a non-governmental organisation representative, 9 July 2020; author interview with a building society representative, 16 July 2020; author interview with a cyber security company representative, 15 September 2020.

With these repercussions in mind, it is not unreasonable for the three areas to be treated as distinct categories of risk for financial institutions. Financial institutions should treat cyber security as a distinct and highly specialised area requiring their attention: legacy infrastructure may be antiquated and ill-suited for cloud-enabled environments.[47] However, insofar as intelligence and investigations are concerned, there are benefits to be drawn from integrating the information collected for cyber security, fraud prevention and anti-money laundering/counterterrorist financing (AML/CTF) purposes. This theme is explored further in Chapter III.

Cyber Security and Technology Companies

Cyber fraud is a volume crime. Therefore, in tackling cyber fraud, 'the more you can prevent the better'.[48] The non-government stakeholders listed in Table 4 are crucial to the prevention effort. Their potential contribution includes reducing the risk of cyber breaches through better cyber security and risk management, removing malicious domains and malware from the internet, building safer services and products for users, and enriching the cyber threat intelligence available to investigators of cybercrime generally. But they also face the trade-off between detecting crime and prioritising functionality and accessibility, with some stakeholders – such as social media platforms – having been accused of erring too much on the side of ensuring ease of use.[49] With the participation of stakeholders listed below, programmes such as the NCSC's Active Cyber Defence (ACD) could be enhanced greatly. ACD 'intends to protect the majority of the UK from the majority of the harm from the majority of the attacks the majority of the time'.[50] This reflects the notion that cleaning up the internet should not be solely the government's responsibility, and more active engagement with the stakeholders listed below would have a significant impact for users.

47. Author interview with a cyber security company representative, 16 July 2020.
48. Author interview with an information-sharing platform representative, 21 July 2020.
49. Author interview with a law enforcement officer, 29 July 2020.
50. NCSC, 'Cyber Strategy Update Shows How UK Intelligence Is Thwarting Attack', 16 July 2019, <https://www.ncsc.gov.uk/news/active-cyber-defence-report-2019>, accessed 6 November 2020.

Table 4: Cyber Security and Technology Stakeholders

Organisation	Current Role	Issues with Current Activity
Internet service providers (ISPs)	Direct and clean internet traffic through Deep Packet Inspection;* block content for copyright infringement (for example, IP blocking, blocking by DNS redirection);† share intelligence among ISPs and with UK government agencies.	Balancing privacy concerns for users and avoiding 'the Great Firewall of the UK';‡ lack of incentives beyond good will or limited formal frameworks; strong relationships between ISPs, but little intelligence sharing with wider industries or law enforcement agencies; ad-hoc engagements are particularly difficult for ISPs due to the lack of scalability in their internal systems.§
Cyber threat intelligence	Collect and analyse cyber threat intelligence; intelligence sharing with law enforcement agencies.‖	Collaboration is based on good will or marketing opportunities, making it ad hoc; lack of incentive model to engage in further activity such as takedowns.
Managed security service providers	Defend organisations from cyber attacks/breaches and assist in incident response; provide cyber threat intelligence-led defence for clients; assist in cyber awareness at the organisational level via tools and education.	They are primarily there to serve organisations in defending their networks and so do not perceive a stake in the cyber fraud model.
Registrars	Register domain names for businesses and individuals; take down malicious domains when requested.	There is little consistency in approach among smaller registrars; inconsistent desire to take down a domain, particularly internationally; lack of evidence of criminal activity to take down the domain; some, not all, lack engagement to meet responsibilities.
CERTs (Computer Emergency Response Teams) and CSIRTs (Cyber Security Incident Response Teams)	Active defence of national cyber security; collect and analyse cyber threat intelligence; can influence the activity of ISPs.¶	Inconsistent cooperation.**

Organisation	Current Role	Issues with Current Activity
Social media companies and online marketplaces	Assist in prevention of fraud through their platforms; remove malicious links and advertisements; provide intelligence to law enforcement investigations.	Inconsistency both in removing malicious links and ads and in assisting law enforcement investigations.[††]
Large technology companies, telecommunication providers and online service providers (other than those listed above)	Can provide support to cybercrime investigations or, in rare cases, participate in technical disruption operations.[‡‡]	Proactive engagement depends on the company's goodwill (and, in all likelihood, the perceived impact on its reputation).

Sources: [*] 'A network packet is a formatted and discreet unit of data. Deep packet inspection is a method of analysis that dissects network data to extract useful metadata'. See Dan Patterson, 'Deep Packet Inspection: The Smart Person's Guide', TechRepublic, 9 March 2017, <https://www.techrepublic.com/article/deep-packet-inspection-the-smart-persons-guide/>, accessed 6 November 2020; [†] Ofcom, 'Online Content Study: Changes in the Distribution, Discovery and Consumption of Lawful and Unauthorised Online Content', March 2016, p. 52. ISP site blocks have had a significant impact on all blocked sites analysed for the UK, with all categories showing a significant decline in usage; [‡] Author interview with a multinational bank representative, 23 July 2020; [§] Author interview with a policy officer at an ISP, 23 September 2020; [‖] Author interview with a law enforcement officer, 14 July 2020; [¶] Author interview with a fraud technology specialist at a technology provider, 6 August 2020; [**] Author interview with a fraud technology specialist at a technology provider, 6 August 2020; [††] Author interview with a multinational bank representative, 23 July 2020; [‡‡] In the US, in October 2020, Microsoft obtained a court order requiring a hosting service provider within the US courts' jurisdiction to halt the provision of services to persons operating the Trickbot botnet, which was used to distribute malware. See Microsoft, 'New Action to Combat Ransomware Ahead of U.S. Elections', 12 October 2020, <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/>, accessed 6 November 2020.

In the case of the stakeholders outlined in Table 4, the architecture of technology and the internet is another consideration, but one that is beyond the scope of this paper. Nonetheless, the current ecosystem is lacking incentives to engage stakeholders at a deeper level in tackling cyber fraud.

The overarching question in tackling cyber fraud is how to do so effectively in view of the significant reliance on private sector actors.[51] Coordinating with a large variety of groups with different aims or interests remains a challenge for policymakers.

Information-Sharing Arrangements

There are two basic modes of sharing information relevant to preventing, detecting and investigating cyber fraud. The first is compliance by businesses with their reporting obligations

51. Author interview with a non-governmental organisation representative, 13 July 2020.

under various applicable laws, as mentioned in Table 3. Such reports go one way (from reporting businesses to the government) once the requirement to report has been triggered. The second is participation in information-sharing partnerships. These are more likely to involve a mutual information exchange and be voluntary in nature. Due to the sensitivity of information being shared, they may rely heavily on trust and be difficult to expand. Trust is also related to the boundaries of sharing as per the General Data Protection Regulation (GDPR), highlighted by several research participants as a reason which – irrespective of its limitations in certain law enforcement contexts – is often used to draw back from sharing important information.[52]

Reporting by the Private Sector

Private sector reporting[53] mandated by the law includes two main mechanisms: suspicious activity reports (SARs) and financial crime reports.[54]

A regulated business must submit a SAR if it has 'reasonable grounds for knowing or suspecting' that a customer is engaged in money laundering.[55] If the regulated business is asked to carry out a transaction that would amount to money laundering, it can file what is colloquially known as a 'defence against money laundering' SAR to request the NCA's consent to proceed with the transaction.[56]

The operation of the UK's SAR regime is a subject central to the UK's response to economic crime, including fraud. Over 478,000 SARs were submitted between April 2018 and March 2019.[57] SARs have a dual function of alerting law enforcement agencies to possible crime and forming the contents of a SAR database that can be searched as and when the need to do so arises. However, the quality of SARs is uneven,[58] and the UK Financial Intelligence Unit's ability to analyse them is subject to ongoing reform.[59]

52. Author interview with a UK insurance company representative, 23 July 2020; author interview with a representative of an information-sharing organisation, 21 July 2020; author interview with a small bank representative, 30 July 2020; author interview with an industry association representative, 23 July 2020; author interview with an NGO representative, 9 July 2020.
53. A November 2019 Treasury Committee report into economic crime raised concern that 'banks do not always appear to be reporting instances to the police where, for example, the bank has reimbursed the victim' and that 'the Government should require all frauds to be reported regardless of their size, and whether or not a financial institution has reimbursed a consumer'. See parliament.uk, 'Investigating Fraud as a Crime', <https://publications.parliament.uk/pa/cm201919/cmselect/cmtreasy/246/24607.htm#_idTextAnchor049>, accessed 6 November 2020.
54. This analysis does not include Action Fraud, which is a crime-reporting avenue for victims.
55. See Proceeds of Crime Act 2002, Section 330.
56. See Proceeds of Crime Act 2002, Sections 327(2)(a), 328(2)(a), 329(2)(a) and 335.
57. NCA, 'UK Financial Intelligence Unit: Suspicious Activity Reports Annual Report 2019', 2019, p. 4.
58. Author interview with a law enforcement agency officer, 29 July 2020.
59. See RUSI Economic Crime Plan Online Tracker, 'Action 30: Deliver First Tranche of SARs IT Transformation and Design the Target Operating Model for the Future of the SARs Regime',

Banks and certain other financial institutions (such as building societies) are also required to submit annual financial crime reports to the FCA that include information on the most prevalent types of fraud faced by the firm.[60] The FCA's only publicly available analysis of financial crime report submissions was published in November 2018 and cited identity fraud and phishing as the most prevalent types of fraud.[61] In July 2020, the FCA launched a consultation on extending financial crime report obligations to a broader range of FCA-regulated businesses, including crypto-asset service providers.[62]

Information-Sharing Partnerships and Industry Forums

The limitations of one-way reporting by the private sector have prompted the emergence of various information-sharing partnerships as summarised in Table 5.

<https://www.rusi.institute/ecp/>, accessed 20 October 2020.

60. FCA, 'Extension of Annual Financial Crime Reporting Obligation', August 2020, <https://www.fca.org.uk/publication/consultation/cp20-17.pdf>, accessed 6 November 2020.
61. FCA, 'Financial Crime: Analysis of Firms' Data', November 2018, <https://www.fca.org.uk/publication/research/financial-crime-analysis-firms-data.pdf>, p. 8.
62. FCA, 'Extension of Annual Financial Crime Reporting Obligation'.

Table 5: Information-Sharing Partnerships and Industry Forums

Platform	Role
Cyber Defence Alliance (CDA)	The CDA brings together eight UK banks* to share information on cyber security and related financial crime threats. Its work covers: the sharing of cyber threat intelligence; facilitating incident response; liaising with law enforcement; and strategic analysis of future threats.
Cyber Security Information Sharing Partnership (CiSP)	The CiSP is administered by the NCSC and includes thousands of UK organisations 'responsible for the administration of an electronic communications network in the UK'.† It covers multiple sectors, including heavy representation from financial institutions. It is solely focused on cyber defence and incident prevention and does not support investigations.
Financial Crime Alerts Service (FCAS)	The FCAS is run by UK Finance to disseminate JMLIT and NFIB intelligence alerts to a broader range of financial institutions.
Joint Fraud Taskforce (JFT)	The JFT, which is chaired by the Home Office, brings together policymakers, law enforcement agencies and private sector representatives such as financial institutions and telecoms companies. Its work is focused on strategic issues such as improving the understanding of both the threat and the 'strategic disruptive response to fraud'.‡
Joint Money Laundering Intelligence Task Force (JMLIT)	The JMLIT shares operational intelligence and publishes intelligence alerts. It consists of an operational group and several expert working groups dedicated to exploring specific risk areas. The legal basis for JMLIT's operations is Section 7 of the Crime and Courts Act 2013, which authorises regulated entities to make disclosures to the NCA.
Virtual Task Force (VTF)	The VTF is convened on an ad-hoc basis by the NCCU to obtain information from retail banks in relation to cases under investigation.

*Sources: * See the biography of Steven Wilson, chief executive officer of Cyber Defence Alliance, at <https://banking.live.ft.com/agenda/speakers/708455?widget=true>, accessed 6 November 2020; † NCSC, 'Cyber Security Information Sharing Partnership (CiSP)', updated 20 March 2018, <https://www.ncsc.gov.uk/cisp>, accessed 6 November 2020; ‡ JFT, 'Our Mission', <https://www.jointfraudtaskforce.org/our-mission>, accessed 6 November 2020.*

Furthermore, public authorities can share information with designated anti-fraud organisations, which include private companies, under the Serious Crime Act 2007.[63] Given the multiplicity of existing information-sharing arrangements, ensuring their complementarity and preventing duplication is vital.[64]

There are also several organisations that play a significant role in disseminating information relevant to cyber fraud detection and prevention in the UK, as summarised in Table 6.

Table 6: Organisations that Disseminate Information Relevant to Cyber Fraud Detection and Prevention in the UK

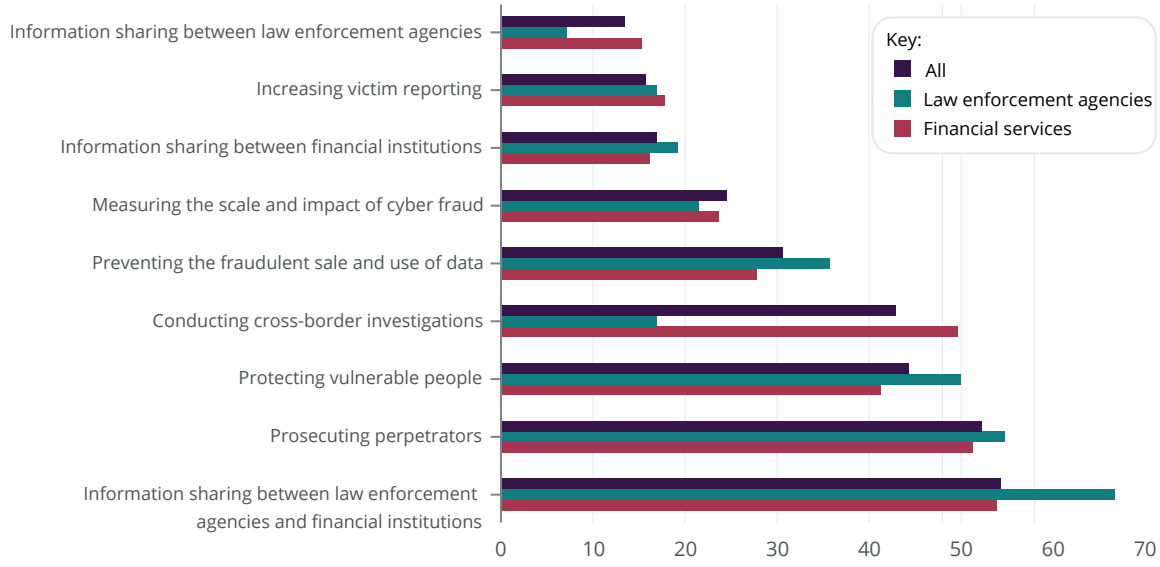
Organisation	Role
Cifas	Cifas is a UK non-profit anti-fraud organisation with over 400 members and participation from government agencies such as the Home Office.* It maintains the National Fraud and Internal Fraud databases, and publishes reports based on the data it holds.
Global Cyber Alliance (GCA)	The GCA is a non-profit organisation founded by the Manhattan District Attorney's Office, City of London Police and the Centre for Internet Security. Its work includes developing free cyber security toolkits.†
UK Finance	UK Finance represents 250 financial firms, and also: performs research and advisory functions; possesses expertise beyond economic crime; funds a Dedicated Card and Payment Crime Unit; shares information on threats through the Economic Crime Information and Intelligence Unit; and conducts training.

*Sources: * Cifas, 'What is Cifas?', <https://www.cifas.org.uk/about-cifas/what-is-cifas>, accessed 6 November 2020; † Global Cyber Alliance, <https://www.globalcyberalliance.org/>, accessed 6 November 2020.*

In conclusion, the range of stakeholders involved in tackling cyber fraud in the UK is broad, as is the breadth of challenges they face. As shown in Figure 4, when asked to list the three most significant challenges in tackling cyber fraud overall, information sharing between law enforcement agencies and financial institutions was the most common response (54% of respondents listed this in their top three), followed by prosecuting perpetrators (52%) and protecting vulnerable people (44%).

63. Serious Crime Act 2007, Section 68.
64. Author interview with a law enforcement officer, 5 August 2020.

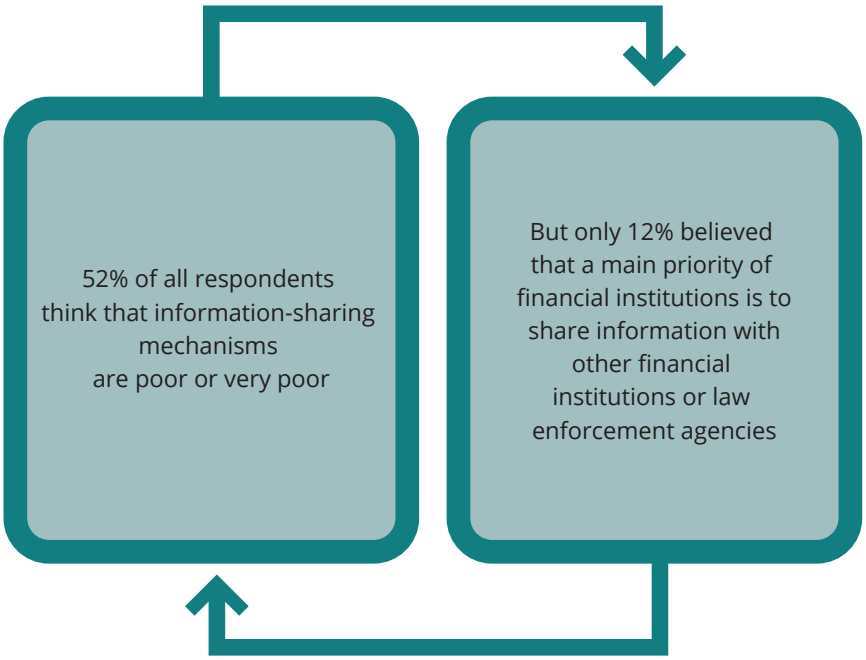
Figure 4: In your view, what are the most significant challenges overall in tackling cyber-enabled fraud in the UK?



Source: Survey data.

Across many of those challenges, private sector companies can and do play a role, not least by participating in public–private information-sharing partnerships. However, each of the existing partnerships come with limitations that relate either to their membership or to the scope of information they share. More importantly, the number of stakeholders involved has not translated into an improvement of the overall effectiveness of the UK's response to cyber fraud. Figure 5 reveals a vicious cycle between expectations around information sharing and current performance.

Figure 5: Prioritising Information Sharing is Problematic



Source: Survey data.

In sum, this chapter has outlined the breadth and scope of the current stakeholders involved in tackling cyber fraud in the UK. The challenges connecting this ecosystem are numerous, especially when existing mechanisms to share information struggle under the volume of the threat. Effective incentives are lacking to encourage further private sector involvement, while policing faces a constant battle against criminals from all corners of the globe. With this context in mind, the following chapter will propose ways to strengthen the UK response.

III. Strengthening the Response

THE CURRENT RESPONSE to cyber fraud in the UK forms a mosaic of actors and initiatives, which is only coherent if every stone is carefully put in its place. Based on the central theme of coordination and incentivisation, this chapter considers: the optimal division of roles and responsibilities for tackling cyber fraud, with emphasis on aligning public and private sector priorities; government and law enforcement activities, ranging from laying out a strategic vision of the response to international engagement; and private sector contribution, ranging from better threat analysis in the financial sector to a consideration of greater partnerships with technology companies in cooperative takedowns of criminal infrastructure.

Roles and Responsibilities in a Crowded Space

To illustrate gaps in the current system, it is helpful to imagine a coherent, well-coordinated and effective law enforcement response to cyber fraud. Based on interviews conducted for this project and the authors' analysis, its key features could be summarised as in Table 7.

Table 7: Features of an Effective System of Response to Cyber Fraud

Feature	How It Would Work	Current Shortcomings
Provision of information to law enforcement	Industries with information helpful for law enforcement purposes – including but not limited to financial institutions, ISPs and cyber security firms – would have available to them a pathway to submit information to law enforcement agencies. This pathway would have the following features: 1. **Permanence**, i.e. being used on a more than ad-hoc basis. 2. **Scalability**, i.e. being used by a large number of organisations. 3. **Two-way nature**, i.e. enabling both private-to-public and public-to-private information sharing. 4. **Multi-functionality**, i.e. enabling the sharing of information not only for the purpose of preventing cyber attacks – which is the current focus of CiSP – but also to facilitate the investigation of threat actors behind them.	Both the processes and the quality of information provided to law enforcement have significant deficiencies. None of the current information-sharing partnerships fulfil these four criteria.

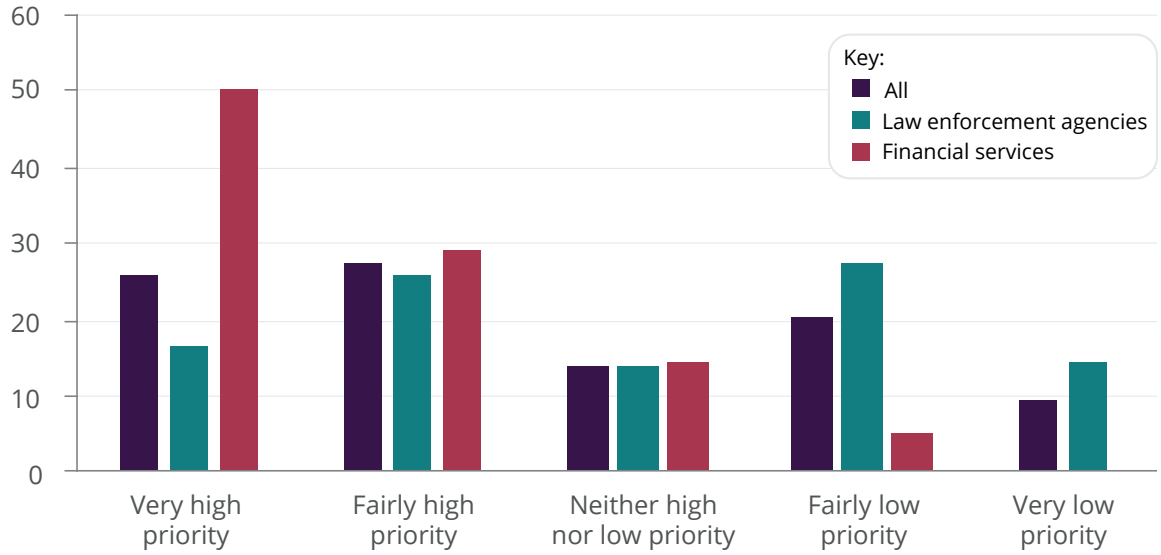
Feature	How It Would Work	Current Shortcomings
Law enforcement activity	Law enforcement agencies would:	Despite progress being made, the following deficiencies remain:
	1. **Analyse**: Access the information they receive from the private sector and aggregate it with other relevant information from law enforcement or government agencies and public sources.	Although the National Data Exploitation Capability (NDEC) housed within the NCA is already reported to be helpful,* the focused analysis of fraud-related data is hampered by the multitude of competing priorities that the NDEC contends with.†
	2. **Investigate**: Conduct investigative activities to identify high-value targets, especially those with a UK nexus (e.g. key individuals, their assets, bulletproof servers, non-AML/CTF compliant virtual asset service providers, dark web marketplaces etc).	The allocation of cases to fraud units is not always consistent, which means complex investigations may not end up within the responsibility of those with the best skills to address them.‡
	3. **Enforce**: Carry out law enforcement operations to apprehend or disrupt the operations of such high-value targets.	The difficulties of enforcement include: relying on the cooperation of foreign countries; the complex and time-consuming nature of investigations; and differences in legislative frameworks.
	4. **Engage**: Disseminate analysis of risks affecting various sectors of the economy across respective industries to inform their defence and risk mitigation measures.§	Although the coronavirus pandemic has seen greater sharing of threat and trend information via JMLIT, the Joint Fraud Taskforce, UK Finance and Cifas, challenges remain in ensuring this information reaches a broad enough range of stakeholders and can be maintained in the future.‖
	5. **Educate and leverage**: Build partnerships with other actors such as ISPs, registrars and cyber security companies to build a complete threat picture.¶ Coordinating on sharing threat intelligence and conducting cooperative takedowns where deemed necessary.	There is insufficient consistent coordination between actors who play parts in tackling cybercrime.** There is a patchy view of the threat landscape.†† Cyber awareness among potential business victims is particularly lacking. It is believed that the regional Cyber Resilience Centres help.‡‡

*Sources: * Author interview with a law enforcement professional at a ROCU, 29 July 2020; † Author interview with a law enforcement officer, 27 August 2020; ‡ Author interview with a UK bank representative, 7 August 2020; author interview with an information-sharing organisation, 22 July 2020; § Author interview with a representative of an information-sharing organisation, 22 July 2020; author interview with a representative of an industry association, 23 July 2020; ‖ Author interview with a law enforcement officer, 27 August 2020; author interview with a multinational bank representative, 23 July 2020; ¶ Author interview with a representative of an information-sharing organisation, 21 July 2020; ** Author interview with a representative of an information-sharing organisation, 22 July 2020; †† First workshop, 27 October 2020; ‡‡ One example is the Cyber Resilience Centre for Greater Manchester. See <https://www.cyberresiliencecentre.com/>, accessed 6 November 2020.*

Aligning Public and Private Sector Priorities

There is a significant difference in how stakeholders perceive and prioritise cyber fraud in their own organisations.[65] This was borne out in findings from the survey data which showed that only 41% of law enforcement respondents listed cyber fraud as either a 'very high' or 'fairly high priority', with 27% considering it a 'fairly low priority'. This stands in stark contrast to the 79% of financial services respondents who considered combating cyber fraud as either a 'very high' or 'fairly high priority' in their organisation. A chi-square test of independence showed that this difference was statistically significant.[66]

Figure 6: To what extent is combating cyber-enabled fraud considered a high priority in your organisation?



Source: Survey data.

65. Author interview with a representative of an industry association, 11 September 2020; author interview with a law enforcement professional at a ROCU, 5 August 2020.
66. X^2 (1, N = 161) = 17.37, p = <0.01.

The knock-on effect of this is that communication between stakeholders can be difficult and misalignment between actors may occur. Those interviewed were not always unanimous on whether law enforcement priorities should primarily follow the 'pursue' function outlined by the 4P approach.[67] For commercial organisations – financial institutions and cyber security stakeholders – the main priorities are retaining reputation and money.[68] Research for this paper found that there is some optimism in better aligning law enforcement with stakeholders, but there are still improvements to be made.[69]

Reputational damage from cyber risk was a common theme throughout our interviews.[70] 'Cyber security is not about reduction of fraud, but about the level of integrity and the security of the underpinning architectures of digital society'.[71] This implies that for much of the private sector, outside of financial services, 'cyber fraud' is not the priority – cyber security is.

While businesses are concerned with the reputational damage and loss of profit from cyber incidents and frauds, law enforcement agencies focus on enforcement. Banks are particularly concerned with an 'acceptable risk rate' for fraud, ensuring that the cost of fraud does not go beyond their risk tolerance.[72] This is a key tension in the relationship between law enforcement agencies and commercial organisations in trying to find common ground to form partnerships beyond mere good will. A common finding throughout the research is that this tension is still highly relevant.[73]

One method of reconciling the different perceptions in risk tolerance is to attempt to find common metrics to use within partnerships between financial institutions and law enforcement agencies on cyber fraud. For instance, fraud loss avoidance is a metric used by financial institutions.[74] This could be used by law enforcement as a tool for highlighting progress or success in a reduction of victims – how much money was saved from being stolen.

67. The 4P approach refers to 'pursue(ing)' criminals, 'prepare(ing)' for threats, 'protect(ing)' the public from harm, and 'prevent(ing)' people from engaging in crime.
68. Author interview with a law enforcement professional at a ROCU, 5 August 2020.
69. *Ibid.*
70. Author interview with an NGO representative, 9 July 2020; author interview with a law enforcement professional at a ROCU, 5 August 2020; author interview with a UK insurance provider representative, 23 July 2020; author interview with a representative of an industry association, 11 September 2020; author interview with a representative of a cyber security company, 16 July 2020; author interview with a fraud specialist at a small bank, 30 July 2020; author interview with a law enforcement officer, 4 September 2020.
71. Author interview with an NGO representative, 9 July 2020.
72. Author interview with a law enforcement officer, 29 July 2020; author interview with a law enforcement officer, 6 August 2020.
73. Author interview with a law enforcement professional at a ROCU, 5 August 2020.
74. Author interview with a multinational bank representative, 23 July 2020.

Focusing more on disruption for law enforcement opens the door to wider key performance indicators (KPIs) beyond arrests.[75] Assigning a monetary value to the efforts in disruption to present money saved nationally or internationally is a method of presenting the data similarly to fraud loss avoidance.[76] While the general public may not understand what significant reduction of harm a botnet takedown would create, they are much more likely to understand loss prevention in monetary terms. Furthermore, actors typically not engaged in technical takedowns and proactive defence would further understand this as beneficial to their fraud loss avoidance figures. Law enforcement agencies must stress more qualitative measures of performance as opposed to quantitative. For example, more resource-intensive outcomes should be recognised and weighted.[77]

Another incentive to tackle misalignment is to market successful joint operations more.[78] On the precarious balance of aligning law enforcement drivers with the private sector, one interviewee noted that 'the need for commercial recognition or marketing value can sometimes conflict with the law enforcement need to keep ongoing investigations under wraps'.[79] Aligning action with private sector partners, particularly in disruptive measures, is essential in getting their buy-in.[80] It allows commercial organisations to market the part they played in an operation, thus gathering crucial reputational kudos from clients and peers alike.[81]

Government and Law Enforcement Activities

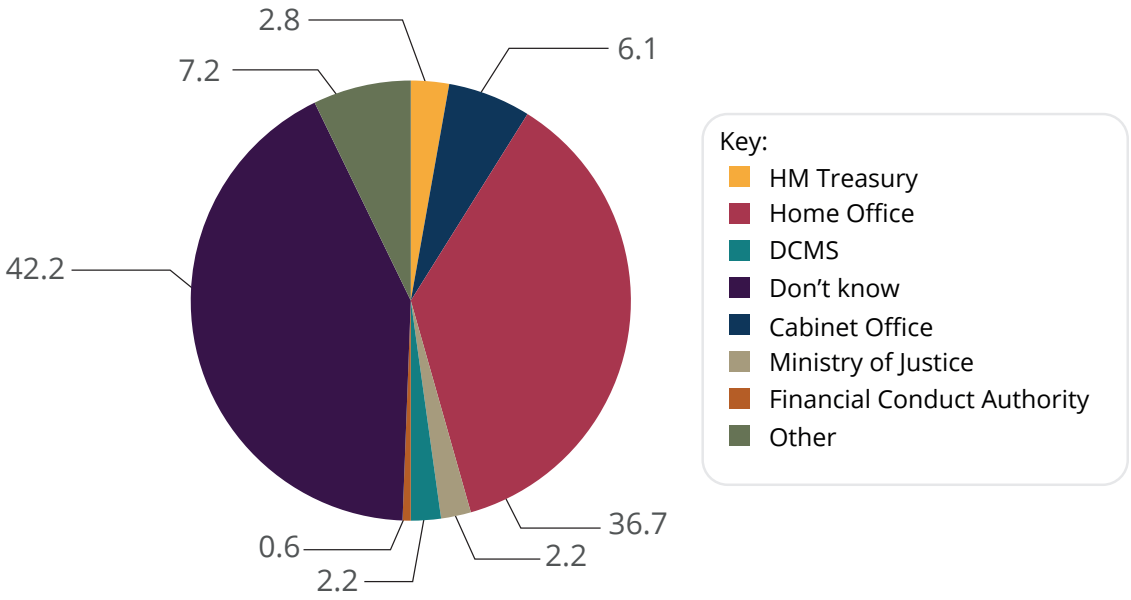
Strategy

There is a distinct lack of coordination or cohesive model for all stakeholders to collaborate on and set terms of engagement. Survey data supports this claim. When asked which government department or agency currently leads on policy development relating to cyber-enabled fraud, the

75. Author interview with a law enforcement officer, 10 September 2020. One participant suggested that 'performance has to be qualitative as opposed to quantitative. Resource-intensive performance outcomes have to be recognised'. Author interview with a law enforcement officer, 29 July 2020.
76. Author interview with a law enforcement officer, 10 September 2020.
77. Author interview with a law enforcement officer, 29 July 2020.
78. Author interview with a representative from a cyber security company, 9 July 2020.
79. *Ibid.*
80. One example of this is the US Department of Justice operation into arresting those behind a Twitter hack. They worked with Chainalysis and Excygent, as well as several national and international actors. See US Department of Justice, 'Three Individuals Charged for Alleged Roles in Twitter Hack', press release, 31 July 2020, <https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack>, accessed 6 November 2020. Another example can be found at US Department of Justice, 'Global Disruption of Three Terror Finance Cyber-Enabled Campaigns', press release, 13 August 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>, accessed 6 November 2020.
81. Second workshop, 29 October 2020.

largest proportion of respondents (42%) reported that they do not know. At the same time, 37% listed the Home Office, while a much smaller proportion listed other government departments, such as the Cabinet Office and HM Treasury, illustrating a concerning lack of clarity among key stakeholders regarding central leadership on cyber fraud policy.

Figure 7: In your view, which government department or agency currently leads on policy development relating to cyber-enabled fraud?



Source: Survey data.

This paper identifies several areas where strategic direction is needed from the UK government, which would ideally be provided in a single document that relevant stakeholders could refer to. Based on both primary and secondary research conducted for this paper, the Home Office is best positioned to take responsibility of this as the government department responsible for security and policing in the UK. This was particularly apparent in survey findings, which showed a majority of respondents (52%) believe that the Home Office is the government department or agency that *should* lead on cyber fraud policy development.

This strategy should be drafted in close consultation with key law enforcement agencies. This should allocate roles and responsibilities to government, law enforcement and industry, and anticipate an important operational contribution from the NCA and the City of London Police. Dissemination and uptake of such a strategy should be actively facilitated by the NECC.

The strategy would ideally address shortcomings in the areas of investigation and enforcement, performance measurement, training and resourcing, information sharing, the role of the private sector (including financial services), and victim care and messaging:

1. Reconfigure the 4Ps to the cyber fraud context: include a bigger role for the disruption of technical infrastructure and takedowns in the 'pursue' response – working closely with private sector partners – while ensuring prosecutions and arrests are still prioritised where there is a realistic chance of securing convictions and recovering the proceeds of crime.
2. Develop standardised KPIs for policing which focus less on arrests or judicial outcomes and more on 'protect' and 'prevent' outcomes.
3. Give better clarity on what constitutes lawful information sharing in the cyber fraud space.
4. Commit to ensuring that information-sharing programmes satisfy the four key criteria of permanence, scalability, two-way nature and multi-functionality, thereby upscaling the quantity and quality of data sharing across existing partnerships.
5. More ambitious attempts in the private sector at unifying disparate internal datasets pertaining to cyber, fraud and anti-money laundering, and sharing of examples where this is done effectively.
6. Achieve more transparency and acknowledgement around the role of companies involved in cooperative takedowns of cybercriminal infrastructure with law enforcement.
7. Take bolder action to create pathways where investigators can work across law enforcement and the private sector via national secondment programmes.
8. Ensure that investigative training at the Economic Crime Academy best reflects the practical realities of the intersections between cyber and fraud.
9. Secure resourcing for victim care units so that they reach a wide enough range of the population, underpinned by a more centrally coordinated approach to public messaging.

It is imperative that the strategy be formulated with the specialist teams' leading input,[82] with wider policing leadership feeding in on a more ad-hoc basis.[83] This strategy should complement, not duplicate, the National Cyber Security Strategy, by being able to provide more detail on specific tasking for law enforcement agencies than the National Cyber Security Strategy is able to.

Other measures have also been given due consideration. A new law enforcement agency, for example, could theoretically help coordinate tasking and investigation of cyber fraud cases. Unfortunately, the notion of a new agency solving a myriad of issues in the cyber fraud space ignores the already established and high-potential elements of work from the City of London Police, the NECC and many more. Using the best components of the current model to enhance cooperation and efficiency signals trust in the existing agencies while encouraging more ambitious attempts at partnership and collaboration.

82. These specialist teams include the Proceeds of Crime Centre, the NCSN, the National Economic Crime Academy within City of London Police, and regional coordinators for fraud and cyber.
83. Second workshop, 29 October 2020.

Adjusting the 4P Model for Cyber Fraud

The '4Ps' approach has traditionally been used in the context of counterterrorism[84] and is a central part of the government's Serious and Organised Crime Strategy.[85] These 4Ps refer to:

- **Pursue**. This refers to law enforcement activities which reduce the threat of crime through the investigation of groups and individuals and the disruption of their activities.
- **Prepare**. This refers to ensuring that procedures are in place for mitigating the impact of serious crime.
- **Protect**. This refers to actions which safeguard individuals, organisations and systems from the effects of serious and organised crime.
- **Prevent**. This strand focuses on efforts that stop people from engaging in serious and organised crime in the first instance.

As law enforcement has had to reckon with an increasingly complex and diverse economic crime landscape, it is important to ascertain the transferability of the 4P model to the cyber fraud context, and how priorities and resources should be arranged across those 4Ps. Under this framework, a more coordinated, whole-of-system approach can be activated to manage and respond to the relevant threat. It allows for a clearer delineation of responsibilities between different agencies, bringing into the fold specialist expertise (such as via the NCSC) beyond the traditional law enforcement channels.

The first P – 'pursue' – is one that received the most attention during research for this paper. It has traditionally referred to law enforcement activities which reduce the threat of crime through the investigation of groups and individuals and the disruption of their activities. Yet, one of the main issues with this description is that it affords little distinction between investigation and disruption. These two things were seen as necessarily separate by research participants. As has been established in this paper, cyber fraud investigations often lead to law enforcement authorities chasing assistance from hard-to-reach jurisdictions where many offenders are based. Even when there is a lead on where an offender might be located, turning that information into evidence which can pinpoint their identity and be used in a subsequent prosecution tends to be difficult.

Disruption activities, on the other hand, are less focused on finding and prosecuting criminals, irrespective of where they are located. They are more focused on technical activities which strike at individual components of a criminal infrastructure. In combination, these activities can help minimise criminal gain from cyber fraud and deter future involvement in the crime. Examples will include: dismantling technical architecture, such as servers used to spread spam

84. HM Government, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, Cm 9608 (London: Her Majesty's Stationery Office, 2018).
85. HM Government, *Serious and Organised Crime Strategy*, Cm 9718 (London: Her Majesty's Stationery Office, 2018).

emails; targeting professional enablers in the legal or financial services industry; and interrupting payments in the financial system on their way to criminal accounts.[86]

Disruption activity is not solely in the domain of the police; the NCA and the NCSC are prominent in this area of 'pursue' too. There is also a role for non-government organisations whose purpose it is to tackle cyber risks before they become a reality. One representative commented that '80% of the problem is the reduction of the infrastructure to minimise the harm in the first place. Then, yes, there is a remaining 20% which involves helping the police to catch people'.[87] Other participants warned of the need to not 'abdicate our responsibility', stating that:

> There needs to be fundamental change in how we take the fight to perpetrators. Whether it is state actors, organised criminals or individuals, how far behind are we in terms of taking that fight to them, compared to the things that we do against the drug trafficking trade, for example?[88]

With respect to fraud investigation, several concerns were noted. One is that not enough officers are adequately trained in the Fraud Investigation Model[89] – 'without this model being applied systematically, fraud becomes an unwieldy beast, but SIOs [senior investigating officers] don't always understand this'.[90] Similarly, it is unclear how and when the 'fraud escalation policy'[91] from local force level to ROCU level should be deployed. At the moment, it does not play a significant role when local forces are struggling with the complexities of a case.[92] On cyber investigative skills, technical expertise is specialist and therefore faces different challenges to that of fraud investigations. There is little overlap between the two specialisms that provide a holistic investigative skillset to officers.

These findings are indicative of a concern that the 'pursue' response is currently lacking the support it needs to conduct strategic operations, which pool the various sources of knowledge in cyber and fraud across the enforcement landscape. Strategic direction of the law enforcement

86. See Box 1 for examples of technical takedowns done jointly with policing and technology companies/internet service providers.
87. First workshop, 27 October 2020.
88. *Ibid.*
89. 'The model, in comparison to other investigative models, identifies that criminality, risk of harm and loss continues following reporting and during investigation and data gathering stage … The model considers the need to limit the period of harm and loss by stopping the fraudster at the earliest opportunity, placing an emphasis upon opportunities for early disruption and prevention with initial evidence gathering and data collection'. See Suffolk Police, 'Fraud Allocation and Investigation', <https://www.suffolk.police.uk/sites/suffolk/files/fraud_allocation_and_investigation_draft_internet_version.pdf>, accessed 6 November 2020, p. 11.
90. Author interview with a law enforcement professional at a ROCU, 5 August 2020.
91. Author interview with a law enforcement professional at a ROCU, 29 July 2020. The fraud escalation policy refers to tasking investigations. If an investigation is too complex for a force, they will refer the case to a force with greater capacity.
92. Author interview with a law enforcement professional at a ROCU, 29 July 2020.

'pursue' response is unclear, and this is not helped by the absence of a distinction between investigation and disruption activities.

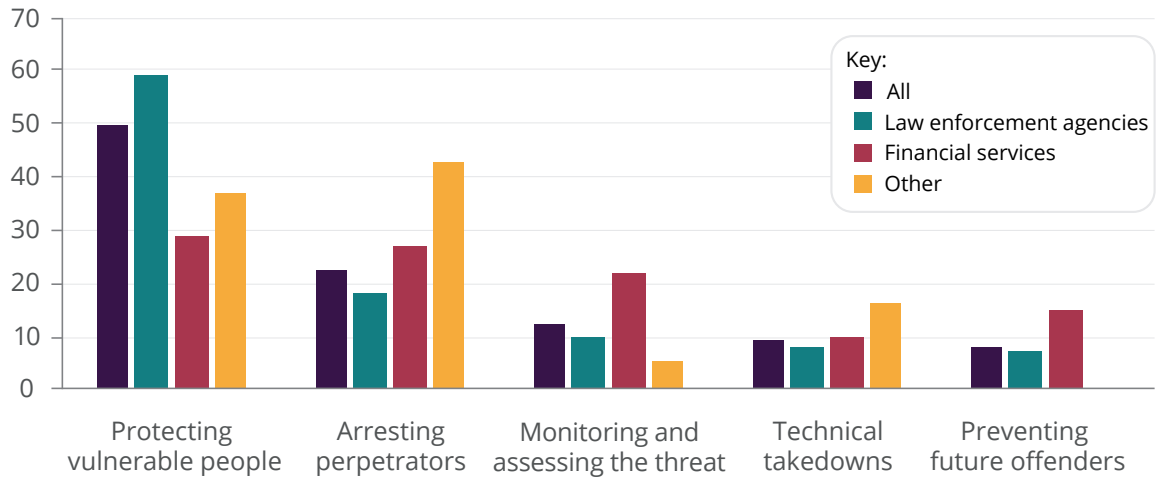
Such a comparison between 'pursue' and 'protect' was regularly made by research participants. Given the large number of people falling victim to cyber frauds every year, ensuring that victims receive a level of service from law enforcement authorities to mitigate the impacts of cyber fraud has become an increasingly important part of the 4Ps response. One law enforcement representative said 'I spend a lot of time doing the "protect" work, but on my own, it is hard to do it justice. My colleagues in cyber in the region have dedicated "prevent" and "protect" officers, so there is a need to try and replicate that model for us too'.[93] Ensuring that ROCUs dealing with local fraud cases have the right level of support to carry out that work should be a 'protect' priority moving forward. Increased resourcing for the National Economic Crime Victim Care Unit to ensure that the service can reach a wider range of residents in more force areas would significantly help.

Survey data reinforces the finding that law enforcement agencies see an important role for themselves in the 'protect' function. As shown in Figure 8, when asked to rank the most important priorities for law enforcement agencies in tackling cyber fraud, the majority of law enforcement respondents (59%) suggested 'protecting vulnerable people' as the top priority. Notably, however, only 29% of financial services respondents agreed.[94] This difference in views suggests that there needs to be a more explicit communication from law enforcement to financial services of the benefits they are bringing to the 'protect' response, sharing best practice and KPIs where possible.

This is brought into sharper relief considering that when respondents were asked to rank the top priorities for financial institutions in combating cyber fraud, 72% of all respondents suggested that the top priority should be to protect customers.

93. First workshop, 27 October 2020.
94. A chi-square test of independence showed that this difference was statistically significant, X^2 (1, N = 161) = 11.37, p = <0.01.

Figure 8: In your view, what should be the most important priority for law enforcement agencies in tackling cyber-enabled fraud?



Source: Survey data.

Figure 9: Protecting Customers and Vulnerable People is Central to Tackling Cyber Fraud

Source: Survey data.

'Prepare' and 'prevent', by contrast, were not mentioned by research participants to the same degree as 'pursue' and 'protect'. One participant went so far as to say that 'there is next to no "prevent" work going on here because we're always having to react to everything'.[95] With the prevailing view that many offenders are based overseas and therefore unreachable for domestic 'prevent' activities, there is a risk that resources dedicated to reaching local populations and deterring involvement in organised criminal networks are severely cut back.

This is also borne out by Figure 8. 'Monitoring and assessing the threat' – which most closely aligns with the 'prepare' function – and 'preventing future offenders' were only ranked as a top priority by respondents 12% and 7% of the time, respectively.

A key part of the 'prepare' response which was prevalent in research interviews – the training and upskilling of investigators – is addressed in more detail below.

95. Author interview with a law enforcement professional at a ROCU, 5 August 2020.

Training and Upskilling

Increasing digitalisation of society creates challenges for policing. In the UK, the need to address them has resulted in the creation of specialist cybercrime teams and a drive to encourage digital investigative skills. However, there exists 'a deceptive separation or exaggerated distinction between cyber and conventional policing'.[96] That 'distinction' could prevent staff and officers from pursuing roles or training in cyber.

Training and upskilling officers to work on specialist crime types, such as fraud or cyber, is an ongoing challenge and, according to interviewees, left largely up to individual forces to insist on.[97] New officers are frequently not trained in the Fraud Investigation Model, which does not form part of the National College of Police Training's requirements.[98] In order to support upskilling in fraud investigations, the NPCC is looking at fraud as part of the student officer training programme.[99]

Another issue is that salaries in policing are not competitive for the level of skill required for cyber investigations.[100] Commonly, police staff[101] – not officers – leave policing because of competitive pay scales in the private sector, leading to a high staff attrition rate. Officers tend to get better pay and benefits for the role, with a lower attrition rate as a result.[102] Still, police officers are not immune to the temptations of higher salaries in the private sector either. However, cyber operations are reliant on specialist skill sets, such as dark web investigations, which are typically filled by police staff, not officers.

To break down siloes and boost interest in investigating cyber fraud, a specialist cyber fraud investigator training programme is needed. This would help in bridging the gaps between financial crime and cybercrime, building a cohort of investigators who are equipped to understand the complex nature of cyber fraud. Tech savvy – but not technical – individuals would find this an attractive option to investigate a harmful crime while also learning more about the cybercrime aspects.

Seconding experts from the private sector (financial services, cyber security and more) is another way to plug the skills gap in fraud and cyber.[103] Various police forces already do second experts

96. Chrisje Brants, Derek Johnson and Tim J Wilson, 'New Wine in Old Bottles: Alternative Narratives of Cybercrime and Criminal Justice?', *Journal of Criminal Law* (Vol. 84, No. 5, October 2020), p. 403.
97. Author interview with a law enforcement professional at a ROCU, 5 August 2020; author interview with a law enforcement professional at a ROCU, 29 July 2020.
98. Author interview with a law enforcement professional at a ROCU, 5 August 2020.
99. Author interview with a law enforcement professional at a ROCU, 29 July 2020.
100. Author interview with a representative of an industry association, 11 September 2020.
101. That is, professional support staff working in law enforcement agencies who do not have the rank of a police officer.
102. Author interview with a law enforcement professional at a ROCU, 5 August 2020.
103. Author interview with a representative of a cyber security company, 9 July 2020.

in for roles, but this is not a widespread or formalised practice.[104] Simultaneous to seconding in experts from other sectors, offering graduates attractive opportunities to upskill in cyber, fraud and digital policing could facilitate developing in-house expertise.[105] Finally, paying police staff with specialist skills a more competitive salary, at least in line with officer pay scales, would help to prevent high attrition.

Legislative and Regulatory Changes

There are several issues with current legislation to tackle cyber fraud and wider cybercrime. The Computer Misuse Act 1990 (CMA 1990) is one such example. It has long been critiqued for criminalising legitimate penetration testing activities by virtue of not requiring any criminal intent or harm to the victim.[106] Penetration testing activities are often carried out by cyber security companies as part of their services for wider industry to help find vulnerabilities and fix them in a company's network. They therefore play an important part in the cyber resilience of businesses. This issue is ripe for re-examination given the deterrent effect that the current wording of the CMA 1990 may have on bolstering organisations' cyber resilience.

There are also criminal justice-related issues with the CMA 1990. Currently, there are a limited number of successful prosecutions under it.[107] However, there is evidence that profit-driven computer intrusions are often prosecuted under other provisions, such as those relating to fraud.[108] There is therefore no way of identifying the number of UK prosecutions and convictions for cybercrime at present. This statistical gap could potentially be remedied by marking prosecutions as involving deception and the use of the internet (namely cyber fraud) for statistical purposes regardless of the offence charged. Gathering such data could facilitate a reappraisal of whether English criminal law is well suited for criminal prosecution of cyber fraud, which is arguably an issue that merits the Law Commission's examination.

Another prominent issue is the unintended consequences of the EU's GDPR and UK Data Protection Act 2018.[109] The main impact has been on commercial organisations – both financial

104. NCA, 'Experienced Professionals', <https://www.nationalcrimeagency.gov.uk/careers/how-to-join-the-nca/experienced-professionals>, accessed 6 November 2020.
105. Author interview with a representative of an industry association, 11 September 2020.
106. Criminal Law Reform Now Network, 'Reforming the Computer Misuse Act 1990 – Full Report', 2020, p. 64, para. 4. 22.
107. A possibly not comprehensive but helpful database of Computer Misuse Act 1990 cases based on public sources is available at Computer Evidence, 'Computer Misuse Act 1990 Cases', <https://www.computerevidence.co.uk/Cases/CMA.htm>, accessed 6 November 2020.
108. Author interview with a fraud specialist at a building society, 16 July 2020; author interview with a law enforcement officer, 29 July 2020; author interview with a law enforcement officer, 29 July 2020.
109. Author interview with a representative of a UK insurer, 23 July 2020; author interview with a representative of an industry association, 11 September 2020; author interview with a policy officer at an information-sharing platform, 21 July 2020; author interview with a law enforcement officer, 22 July 2020; author interview with a fraud investigator at a small bank, 30 July 2020;

institutions and cyber security companies – and their willingness to share. GDPR has created a culture of fear of disclosure, making intelligence sharing with law enforcement agencies difficult beyond the established formal reporting procedures like the JMLIT. To fully exploit the intelligence potential of the private sector, the Information Commissioner's Office should set out guidance clarifying under what circumstances and using what channels businesses can lawfully share intelligence with government and law enforcement agencies without fear of breaching data protection legislation. Moreover, the sharing of anonymised intelligence does not raise any data protection issues, and data protection is not an acceptable excuse to withhold anonymised threat intelligence from law enforcement agencies.

Consideration can also be given to regulation aimed at bringing actors on the periphery of the ecosystem into the fold,[110] such as placing a duty on social media platforms to detect and take down fraudulent advertisement or malicious links.[111] Another example would be to force ISPs to share intelligence with law enforcement agencies. This would greatly reduce the number of people that fall victim to false adverts or malicious links being hosted on their platforms. Regulation, however, should be viewed carefully, as it can be costly and prohibitive to enforce not just for companies, but for government too.

Messaging

An effective defence in tackling cyber fraud is good cyber literacy among individuals and within businesses.[112] Because the impact of financial harm to individuals and businesses can be life-changing and economically damaging to society, it is particularly important to prevent individuals and businesses from being defrauded in the first place.[113] Good cyber hygiene practices include active implementation of simple measures to protect an individual online. The NCSC has a programme for this work called Cyber Aware.[114] It consists of six easy steps for individuals to implement:

1. 'Use a strong and separate password for your email'.
2. 'Create strong passwords using 3 random words'.
3. 'Save your passwords in your browser'.
4. 'Turn on two-factor authentication'.
5. 'Update [the software on] your devices'.
6. 'Back up your data'.[115]

---

author interview with a representative of an industry association, 23 July 2020; author interview with a representative of an NGO, 9 July 2020; second workshop, 29 October 2020.

110. Author interview with a policy officer at an information-sharing platform, 21 July 2020.
111. Author interview with a policy officer at an information-sharing platform, 23 September 2020.
112. First workshop, 27 October 2020.
113. Author interview with a representative of an information-sharing platform, 21 July 2020.
114. NCSC, 'Cyber Aware', <https://www.ncsc.gov.uk/cyberaware/home>, accessed 6 November 2020.
115. *Ibid.*

The NCSC is the lead technical authority responsible for advising what steps people should take. The cyber hygiene campaigns run by policing through their 'protect' work often does and should follow the same guidance. Although there is clear value in educating people on how to protect themselves from cyber fraud, campaigns often exhibit varying levels of efficacy. One participant suggested that financial services firms are more effective at education and awareness.[116] There are several campaigns currently being run aside from the Cyber Aware campaign. UK Finance's Take Five campaign provides people with advice on protecting themselves from being defrauded.[117] The campaign informs them not just of malicious threats online via email, it also tackles social engineering (both digital and physical). However, this suggests a lack of synergy among different, trusted actors running cyber and fraud awareness programmes.

Measuring the impact of cyber and fraud awareness programmes on society is difficult. This makes campaigns hard to justify. One way around this is to focus resources on specific events where cyber fraud is rife, such as Christmas or Black Friday sales. It minimises the cost of persistent advertising and potentially delivers information when people are most vulnerable from fraud.

Once again, technology providers play a huge part in this. Default security settings, underlying vulnerabilities in the architecture of technology and poor cyber security all contribute to the vulnerability of users. Part of the solution is to suggest that companies are regulated to build safer technology in particular ways, such as requiring multi-factor authentication by default on accounts. The other part is for policymakers to establish standards in developing technology, rather than waiting for the private sector to take the initiative. But, within the scope of this research, it can be said that technology providers should be required to take a proactive step in educating their users in basic cyber security. Companies are adept at messaging, and know and understand their users, and they should utilise that knowledge to keep users safe while using their services.

How messaging in the cyber fraud area should address the harm to vulnerable populations remains contested. This is not helped by the conflicting ideas of *who* is vulnerable. Despite the popular idea that the elderly are most likely to be a victim to fraud, an estimated 4.8% of adults aged 65 to 74 and 3.6% of adults aged 75 years and over were victims of fraud in the year ending March 2019, compared with 6.5% and above for all other age groups.[118] The types of fraud where evidence indicates that older people are more likely to be victims tend to represent a smaller proportion of fraud in the Crime Survey for England and Wales, such as lottery scams and investment frauds which are digitally enabled.[119] Work on identifying reliable indicators of

116. First workshop, 27 October 2020.
117. See Take Five to Stop Fraud, 'General Advice', <https://takefive-stopfraud.org.uk/covid-19/general-advice-covid/>, accessed 6 November 2020.
118. ONS, 'Nature of Fraud and Computer Misuse in England and Wales: Year Ending March 2019', 19 March 2020, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#fraud-characteristics-of-victims>, accessed 6 November 2020.
119. *Ibid.*

vulnerability is ongoing. Some noteworthy developments in this area have been driven by the 'CyberSecurity Across the LifeSpan' (cSALSA) research project, which focuses on fatigue and how willpower can be reduced to the point where vulnerability to fraud is high.[120] In reality, different people will be vulnerable to different frauds at different times – vulnerability is not a static concept. These types of considerations should inform more innovative ways of approaching victim care and developing measurements of success that go beyond repeat victimisation.

There should be a recognition that people respond to different messages in different ways. For example, Cyber Aware campaigns tend to be aimed at a younger, more tech-savvy audience where ransomware is more likely to be a concern, whereas the Take Five campaigns are likely to have a slightly older audience where mandate fraud is more relevant.[121] There should be room for both to have a key role in effectively articulating the threat from cyber fraud to the population, and encouraging the constant vigilance required to mitigate that threat. Further, 'protect' messaging for fraud needs centralisation, similar to how the NCSC has centralised its cyber messaging. This would help fraud build a coherent message to potential victims that all other agencies and services can draw upon. The NECC's requisite expertise would match this role well.

International Engagement

The transnational nature of cyber fraud consistently presents challenges for investigation. Some of the most problematic jurisdictions may be hostile to any kind of meaningful engagement, while friendly jurisdictions may have other more pressing enforcement priorities or lack the legal or policy infrastructure to collaborate efficiently.

Establishing national strategic priorities while ignoring the international dynamics of cyber fraud will leave gaps in the response. There are measures that should be taken to ensure this does not happen:

- The first of these is developing a systematic understanding of who the highest-value targets are and where they are located. Investing in this holistic threat picture is a prerequisite for identifying key jurisdictions for engagement.
- Second, the UK should seek to leverage its diplomatic influence to convince other key states (such as those in the Five Eyes alliance) and institutions to prioritise those targets.

A key part of this effort should also be to educate and inform those other jurisdictions of their responsibilities in avoiding international crimes being committed on their territory. One law enforcement interviewee commented:

120. Author interview with a UK government official, 9 September 2020; see cSALSA, 'About the Project', <https://sites.google.com/site/csalsaproject/about-the-project>, accessed 6 November 2020.
121. Author interview with a UK government official, 9 September 2020.

> I often hear from countries that, 'we have no victims here, so we can't really help your investigation'. I then have to say, 'but you have offenders there, and when the money flows back into your country, you'll have money laundering offences there too, you'll also have identities which have been stolen to commit the crimes'. So, it's important how you frame the issue to other regions to make sure they understand it's their problem too.[122]

As well as other states, there are key global law enforcement bodies, such as Interpol, with whom close engagement is essential. Interpol tends to have more open lines of communication with potentially high-harm jurisdictions like Russia and China, who are often inaccessible for UK law enforcement agencies.[123] While using diplomatic influence to name and shame those jurisdictions providing safe harbour for cyber criminals – and following this up with sanctions – is an important part of the UK's international response, it must still be counterbalanced by efforts to use channels like Interpol to achieve closer alignment with hard-to-reach areas.

The UK should also be an active participant of nascent international data-sharing initiatives. There is ongoing work at Interpol to engage private sector companies globally to centralise data and threat intelligence – in 2019, an Interpol resolution announced that '13 temporary agreements have been signed with private companies under the framework of Pilot Gateway, leading to the contribution of important information relevant to cyber-threats, victims and threat actors by private partners'.[124] Subject to necessary data security considerations, UK companies should be part of this and other similar initiatives.

Private Sector Contribution

Threat Analysis in the Financial Sector

As discussed in Chapter II, from the standpoint of financial institutions, cyber security, fraud and financial crime can be treated as three distinct sources of risk. From a criminal perspective, however, these facets of cyber fraud are interlinked. Inefficiencies arise, therefore, if information collected for the purpose of tackling one of these categories of risk is not also used for the other two. Likewise, valuable information may remain unused if one part of the bank interacts with law enforcement without drawing on the data available across the institution.

Some banks have brought together cyber security-, fraud- and financial crime-related information,[125] but the landscape is uneven. Although survey data shows that 52% of financial services respondents believed that functions between cybercrime teams, fraud teams and illicit finance/AML teams were either 'very well coordinated' or 'quite well coordinated' within their organisation, a sizable amount of interview data suggested that responses to these three

122. Comment by a law enforcement interviewee, first workshop, 27 October 2020.
123. Author interview with a law enforcement officer, 10 September 2020.
124. Interpol, 'Resolution No. 11: GA-2019-88-RES-11', <https://www.interpol.int/content/download/14257/file/GA-2019-88-RES-11%20-%20Pilot%20Gateway.pdf>, accessed 29 January 2021.
125. Author interview with a fraud and cyber specialist at a UK bank, 7 August 2020.

areas of risk often remain siloed.[126] This is particularly true in larger institutions that maintain separate hierarchies in various parts of the organisation.[127] Possible models of integration range from increased collaboration between respective units within institutions to their complete integration.[128]

For banks, effectively integrating datasets and trends from across cyber, fraud and AML divisions needs to become a much higher priority. A starting point for this would be to work with industry bodies such as UK Finance to explore ways of exchanging best practice with other banks. The thought of adding regulatory requirements may also be superficially tempting. However, it would be counterproductive to impose an ever-increasing regulatory burden without reasonable certainty that the benefits outweigh the costs.

A moderate first step would be for the FCA to conduct a review of the way in which financial institutions use cyber security-, fraud- and financial crime-related information to form a well-rounded intelligence picture. This review could result in the publication of sanitised examples of best practice and illustrate the benefits that financial institutions could derive from a holistic approach to information that pertains to cyber fraud.

A more direct way of encouraging businesses to do so would be for the FCA to issue public statements that name and praise companies that show best practice. The use of 'regulatory praise' – as opposed to censure – is an underutilised tool in financial crime prevention, and one that may matter to companies.[129] This effort by the regulator could prompt financial institutions to ask themselves the following questions:

- If the institution suffers a cyber attack, is it possible the same threat actor has also stolen money from its customers in other, seemingly unrelated incidents?
- Is it possible that the criminals behind the cyber attack or their money mules are banking with this institution?
- Is it possible that various attacks that the institution has fended off are related?
- What information and expertise does the institution have to bring together to answer these questions?

126. Author interview with a cybercrime specialist at an international organisation, 6 May 2020; author interview with a representative from an information-sharing group, London, 21 July 2020; author interview with an information-sharing platform, 21 July 2020.
127. Author interview with a small bank, 30 July 2020.
128. Salim Hasham, Shoan Joshi and Daniel Mikkelsen, 'Financial Crime and Fraud in the Age of Cybersecurity', McKinsey & Company, 1 October 2019, <https://www.mckinsey.com/business-functions/risk/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity>, accessed 20 October 2020.
129. For instance, one cyber security company referred to the reputational importance of being acknowledged in law enforcement agencies' press releases after rendering assistance to them. Author interview with a representative at a cyber security company, 9 July 2020.

A more ambitious, and in the authors' view necessary, course of action would be for the NCCU, UK Finance, Cifas and City of London Police – prominent coordinating bodies in their respective industries – to bring partners together for a pilot initiative focused on improving the integration of cyber, AML and fraud data. Sanitised examples of best practice in this endeavour should be disseminated via these channels and others like the Joint Fraud Taskforce.

Information Sharing

As summarised in Table 8, none of the existing partnerships fulfil all four criteria of versatility, permanence, scalability and two-way nature that this paper posits as optimal for effective information sharing.[130] This is not a criticism of these partnerships or their effectiveness in achieving their objectives, but a demonstration of how the information-sharing landscape remains fragmented despite the considerable efforts invested in it.

Table 8: Assessment of Existing Information-Sharing Arrangements

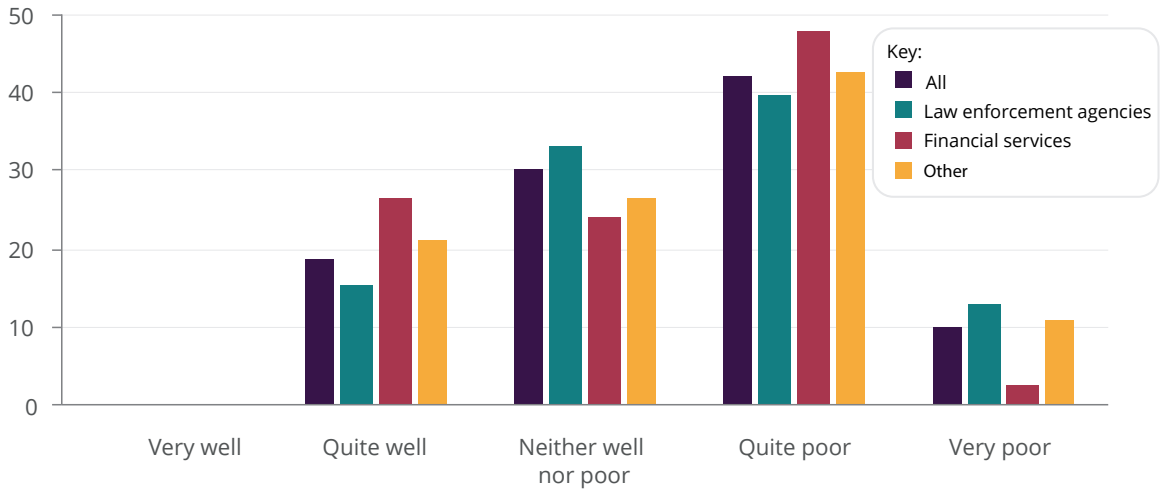
Arrangement	Scalability	Permanence	Two-Way Sharing	Multi-Functionality
CiSP	Yes	Yes	Yes	No*
CDA	No†	Yes	Yes	Yes
FCAS	Yes‡	Yes	No	No
JFT	Yes	Yes	N/A§	N/A
JMLIT	No‖	Yes	Yes	Partly¶
VTF	No**	No	Yes	Yes
Section 68 of the Serious Crime Act 2007	No	Yes	Unknown	Unknown

*Sources: * In practice, CiSP is focused on cyber attack prevention rather than bringing together intelligence that facilitates the investigation of groups that perpetrate them. See references in Anton Moiseienko and Olivier Kraft, 'From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime',* RUSI Occasional Papers *(November 2018), p. 51, which this table is partly based on; † The CDA only includes a limited range of banks; ‡ FCAS disseminates JMLIT alerts to a broader range of financial institutions; § The JFT's work is mostly not operationally focused. See JFT, <https://www.jointfraudtaskforce.org/our-mission>, accessed 6 November 2020; ‖ The JMLIT brings together over 40 financial institutions. See NCA, 'National Economic Crime Centre', <https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed 6 November 2020; ¶ The JMLIT is designed to share financial information but some cyber information, such as IP addresses, are also shared; ** The VTF is convened on an ad-hoc basis and only covers UK retail banks.*

130. These criteria are consistent with outcomes recommended in Nick J Maxwell and David Artingstall, 'The Role of Financial Information-Sharing Partnerships in the Disruption of Crime', *RUSI Occasional Papers* (October 2017), which is based on the analysis of six financial information-sharing partnerships.

The limitations of existing information-sharing mechanisms are also apparent from questionnaire data. When asked how cross-sector information-sharing mechanisms are working in relation to cyber fraud, the majority of respondents (82%) reported that these are not working well. No respondents reported that these are working 'very well', and only 18% suggested these are working 'quite well'. Forty-two percent characterised these mechanisms as 'poor', while 10% characterised them as 'very poor'. Thirty percent responded 'neither well nor poor'.[131] There were no significant differences between cohorts, indicating a consensus among respondents regarding the deficiencies of existing cross-sector information-sharing mechanisms.

Figure 10: How well or how poor do you think existing mechanisms for cross-sector information sharing are working in relation to cyber-enabled fraud?



Source: Survey data.

Given the centrality of information sharing to an effective response to cyber fraud, it is necessary to consider designing information-sharing partnerships that would satisfy the criteria in Table 7. Such partnerships would operate on a permanent basis and be intended to share a broad range of cyber-related information. This is the model pursued in Germany, where the German Competence

131. A significant share of the respondents (30%) described them as 'neither well nor poor'. This is a particularly interesting finding as it may demonstrate how stakeholders find it quite hard to measure the differential impact of these information-sharing partnerships, and the value for the time and money that they input into the process.

Centre against Cybercrime unites 11 banks, insurance companies and cyber security consultancy companies that cooperate with the German federal police.[132]

This could be achieved by developing a new partnership or reforming existing ones. The former option may be unappealing as it will further increase the number of partnerships in an already crowded space with no guarantee of effectiveness. Some interviewees were extremely sceptical about creating a new information-sharing partnership.[133] A better option could therefore be the organic expansion of CiSP's focus to move it beyond the prevention of cyber attacks (although that may not be compatible with its current ethos of a prevention-focused system with minimal law enforcement involvement) or the greater shift of the JMLIT towards sharing information on criminals' digital footprint.

Another essential consideration in the context of cyber fraud is that the reach of partnerships should extend beyond the most sophisticated organisations, such as financial institutions. Otherwise, there is a risk that those organisations will advance even further while other sectors of the economy will be left behind and therefore be less able to defend themselves against cyber risks. CiSP is an example of good practice in extending information sharing across multiple business sectors while the JMLIT has found it difficult to scale up its trust-based model to include participants from outside the financial industry.

In the meantime, the gap in the availability of official information on cyber security- and cybercrime-related trends is being filled by formal and informal private-to-private arrangements, such as those facilitated by industry groups.[134] Some of their participants fear that formalisation and regulator participation would not be helpful and would hamper what is now a free exchange of views.[135] That said, ad-hoc attempts at information sharing do not allow the sharing of operational intelligence and are difficult to maintain in the long run.[136] Such private-to-private sharing can help ascertain whether certain information merits being reported to law enforcement agencies.[137]

Reliance on the private sector raises the question of why companies would give up their time to provide law enforcement agencies with better information. Part of the answer lies in the benefits of this partnership, such as better understanding of the threat picture, only accruing to its participants. This factor is not trivial, as seen by how private-to-private partnerships like the CDA have endured. Businesses are also likely to be drawn towards what is seen as best practice, particularly if they are subject to regulation and therefore willing to impress regulatory authorities. Along with the broader reputational considerations, this is likely to be crucial.

132. German Competence Centre against Cybercrime, 'Vereinsarbeit', <https://www.g4c-ev.de/?page_id=297>, accessed 6 November 2020.
133. Author interview with a fraud and cyber specialist at a UK bank, 7 August 2020.
134. Author interview with a representative from a non-governmental organisation, 5 August 2020.
135. Author interview with a representative from a UK insurer, 23 July 2020.
136. Author interview with a policy officer at an information-sharing platform, 23 September 2020.
137. Author interview with a fraud investigator at a building society, 16 July 2020.

Direct Assistance to Law Enforcement

The most far-reaching mode of public–private partnership is enlisting private sector organisations in investigating cyber fraud. In this context, partnership is distinct from a purely commercial relationship with private organisations that provide investigatory services to governments, such as threat intelligence or blockchain tracing capabilities. It refers to the provision of services or sharing of expertise on a pro bono or otherwise non-market basis. The range of motivations for companies to do so may differ, from social responsibility, to developing their expertise by working on cases of interest to them, to seeking acknowledgement for their help. Some of these motivations may be less acceptable for the government and law enforcement agencies than others, and there is also the risk that excessive reliance on the private sector may hamper the development of requisite in-house capabilities.

A blanket rejection of private sector assistance would deprive the government and law enforcement agencies of a potentially valuable repository of skills, experience and technology. At the policy level, it would run counter to the ongoing attempts to expand and strengthen a variety of public–private partnership avenues as discussed above. There are legal issues to contend with, including data protection rules, but at least some modes of cooperation may already be available, such as secondments of private sector cyber security experts in law enforcement agencies.

It would be valuable to:

- Develop a framework that established principles under which law enforcement agencies may seek cooperation with the private sector outside of existing information-sharing partnerships, and clarify what form this cooperation may take.
- Publish a guide for private sector organisations on how they can help law enforcement agencies in the prevention, detection and investigation of cyber fraud. At a minimum, this guide should focus on financial and cyber security industries.

Cooperative Takedowns and Technical Interventions

Another instance of public–private collaboration is cooperative takedowns, or joint operations by law enforcement agencies and private companies to dismantle cybercrime infrastructures. Takedowns also rely heavily on international agencies and law enforcement in partner countries. The most recent example is the dismantling of Emotet infrastructure, which required international cooperation from the UK's NCA and NCSC, the FBI in the US, and European partners Eurojust and Europol.[138] This case highlights how vital international engagement and healthy partnerships

138. Emotet is malware commonly spread through email spam. See Malware Bytes, 'Emotet', <https://www.malwarebytes.com/emotet/>, accessed 1 February 2021; NCA, 'NCA in International Takedown of Notorious Malware Emotet', 27 January 2021, <https://www.nationalcrimeagency.gov.uk/news/nca-in-international-takedown-of-notorious-malware-emotet>, accessed 1 February 2021.

with other agencies are in cooperative takedowns, as well as private sector partners. Some successful examples of public–private collaboration are listed in Box 1.

To reap maximum benefits from such engagement, it should be formalised as far as possible, providing a platform for more businesses to join relevant operations. The City of London Police and the NCCU, with the NCSC, should lead on the engagement and identify top-level threats that should be targeted. To incentivise the private sector to further engage in cooperative takedowns, it has been suggested that regulation requiring companies to engage in technical takedowns could be considered.[139] But it is unclear who would enforce such regulation and how effective it would be, which is why an approach reliant on companies' voluntary cooperation may be preferable in the short term.

There are significant issues with cooperative takedowns that merit closer inspection. They are said to have a short-term soothing effect on criminal infrastructure and lack engagement and impact in unfriendly jurisdictions.[140] However, this does not negate the benefits of cooperative takedowns acting as a deterrent to crime alongside pursuing and arresting criminals where possible. To induce the private sector to cooperate in takedowns, law enforcement agencies and the NCSC should consider naming companies in their public press releases.[141] It would provide companies with a useful marketing line, boosting their public image with little cost to the government or law enforcement agencies. Furthermore, a potential avenue of engagement with unfriendly jurisdictions is to use private sector partners as proxies for communication. One interviewee noted that it was easier for them, as a bank, to cooperate with law enforcement agencies in unfriendly countries than it was for UK law enforcement.[142] Although this example was about sharing information with the law enforcement agency and not assisting or partnering in a technical takedown, it suggests a new avenue of engagement that can be replicated. Utilising the more neutral image of companies, and particularly financial services firms, is an avenue that should be explored further.

139. Author interview with a professional at a cyber security company, 6 August 2020.
140. For more detail on the specific issues around cooperative takedowns, see Wajeeha Ahmad, 'Why Botnets Persist: Designing Effective Technical and Policy Interventions', Internet Policy Research Initiative, Massachusetts Institute of Technology, 2019, p. 24, <https://internetpolicy.mit.edu/wp-content/uploads/2019/09/publications-ipri-2019-02.pdf>, accessed 6 November 2020.
141. Author interview with a professional at a cyber security company, 9 July 2020.
142. Author interview with a multinational bank representative, 23 July 2020.

Box 1: Examples of Joint Disruption and Takedown Operations

Necurs: A Microsoft-led eight-year operation leading to the takedown of the Necurs botnet, one of the largest botnets in the world.[*] As an example of its impact, one Necurs-infected computer sent 3.8 million spam emails to over 40.6 million potential victims.[†] Partners of the operation included ISPs, domain registries, government CERTs and law enforcement in over nine countries.

Dridex: In 2015, the FBI – with the help of the NCA and private sector partners – took down the Dridex botnet through a court order which saw several command-and-control servers seized. Dridex is a type of banking malware that steals log-in credentials to gain access through several methods. To complete the takedown, law enforcement agencies worked with Trend Micro.[‡]

Ramnit: The European Cyber Crime Centre led an international operation to take down the Ramnit botnet in 2015. Microsoft, Symantec and AnubisNetwords assisted alongside law enforcement agencies from Germany, Italy, the Netherlands and the UK. They collectively dismantled command-and-control servers and redirected 300 domain addresses used by the botnet's operators.[§]

GameoverZeus (GoZeus): In 2014, an FBI-led operation alongside numerous international law enforcement partners and the private sector took down the GoZeus botnet. Private sector partners, including ISPs, helped to clean up malware-infected computers after the servers executing the malware were taken down.[‖]

Sources: [*] Brian Barrett, 'How Microsoft Dismantled the Infamous Necurs Botnet', Wired*, 18 March 2020; [†] Microsoft, 'New Action to Disrupt World's Largest Online Criminal Network', 10 March 2020, <https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/>, accessed 6 November 2020; [‡] Trend Micro, 'FBI, Security Vendors Partner for DRIDEX Takedown', 13 October 2015, <https://blog.trendmicro.com/trendlabs-security-intelligence/us-law-enforcement-takedown-dridex-botnet/>, accessed 6 November 2020; [§] Juan Hardoy, 'Breaking Up a Botnet – How Ramnit was Foiled', Microsoft, 22 October 2015, <https://blogs.microsoft.com/eupolicy/2015/10/22/breaking-up-a-botnet-how-ramnit-was-foiled/>, accessed 6 November 2020; [‖] FBI, 'GameOver Zeus Botnet Disrupted', 2 June 2014, <https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted>, accessed 6 November 2020.*

Further to upscaling technical takedowns, significant issues remain regarding wider cyber security. The first stage in the life cycle – the cyber attack phase – occurs due to insecurity in networks and devices that enable breaches, as well as poor cyber hygiene from users. To tackle the former problem, a series of stakeholders (outlined in Chapter II) would need to be engaged to build a coherent response.

Significant work is ongoing to tackle some of the endemic issues that create vulnerabilities and is part of the UK government's initiative outlined in the National Cyber Security Strategy

2016–2021.[143] For instance, to prevent the insecurity of consumer Internet of Things (IoT) devices, the Department for Digital, Culture, Media and Sport led work to implement standards for IoT manufacturers.[144] At the time of writing, the UK government is currently writing the National Cyber Security Strategy for 2021 and beyond.

The future National Cyber Security Strategy should consider the areas of cyber security policy that greatly undermine the national and economic security of the UK, such as cyber fraud. Cyber fraud is a unique and difficult crime type for law enforcement agencies to tackle alone. While the strategy will help to reduce cyber vulnerabilities across society and build resilience, it should raise the issue of cyber fraud explicitly. By drawing attention to the issue, the dedicated Home Office cyber fraud strategy would segue neatly into the new National Cyber Security Strategy.

143. HM Government, 'National Cyber Security Strategy 2016–2021'.

144. Department for Digital, Culture, Media and Sport, 'Secure by Design', updated 16 July 2020, <https://www.gov.uk/government/collections/secure-by-design>, accessed 6 November 2020.

Conclusion

THE INCREASED RELIANCE of criminals on the internet has transformed how fraud is committed. However, this has not yet prompted a strategic rethinking of the UK's response. This is not to say that no useful steps have been taken to counter cybercrime, including cyber fraud. Helpful measures include: the establishment of the NCSC, the NCCU and cybercrime units in ROCUs; the creation of CiSP and the CDA; and educational campaigns, such as Cyber Aware. But the overall strengthening of the UK's cyber defences has not resulted in a reappraisal of the UK's stance towards cyber fraud specifically.

Cyber fraud now accounts for most of the fraud committed in the UK. It also poses distinct challenges compared to 'traditional', offline types of fraud. They include: the increased need for high-quality digital forensic skills in the investigation of cyber fraud; the virtually unlimited pool of possible offenders from around the world; and the likelihood that – in contrast to the investigation of other types of crime – state-of-the-art expertise and resources may reside in the private sector rather than law enforcement agencies. These challenges call for a response that goes beyond the incremental change that has occurred over the past few years.

Two recent reviews of the UK's measures against fraud and cybercrime respectively have touched on these issues but did not treat them as a focal point for inquiry. A report published by Craig Mackey and Jerry Savill in January 2020 offered recommendations on improving Action Fraud's reporting process and developing specialised investigatory expertise.[145] Meanwhile, the analysis of the UK's response to cyber-dependent crime by Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services in October 2019 contained a relatively modest list of five suggested areas for improvement.[146]

There is, therefore, a need for a new UK strategy dedicated to cyber fraud. Its key themes should be the incentivisation of private sector organisations to support law enforcement and governmental activities and the upskilling of law enforcement agencies. The strategy would outline a restructuring of the current approach to tackling cyber fraud by reviewing all information-sharing partnerships, upscaling technical takedowns as short-term relief and implementing a nationwide secondment programme to bring specialist knowledge into the police. To assist in this, the strategy should reformulate KPIs to reflect more 'protect' and 'prevent' work, bolstering the vital role of law enforcement agencies in all four 'P's, not just two of them.

---

145. 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, pp. 53–54.
146. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, *Cyber: Keep the Light On – An Inspection of the Police Response to Cyber-Dependent Crime* (London: HMICFRS, 2019), p. 21.

Although these recommendations may not eradicate cyber fraud, they will have a marked difference on how the UK mobilises against the problem in the coming years. Criminals will constantly innovate where there is money to be made. It is not an option to stand still in the face of this – there are millions of citizens and businesses depending on swift and assertive action being taken now.

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 in RUSI's Organised Crime and Policing team. His research currently spans numerous areas within organised crime and national security, including the application of emerging technologies for use in national security and law enforcement contexts, the intersections between cybercrime and fraud, and intellectual property crime.

Anton Moiseienko is a Research Fellow in RUSI's Centre for Financial Crime and Security Studies. His research covers a range of subjects that include the laundering of the proceeds of cyber-dependent and cyber-enabled crime and money-laundering vulnerabilities of online businesses.