Royal United Services Institute
for Defence and Security Studies

Occasional Paper

The Silent Threat

The Impact of Fraud on UK National Security

Helena Wood, Tom Keatinge, Keith Ditcham and Ardi Janjeva

The Silent Threat

The Impact of Fraud on UK National Security

Helena Wood, Tom Keatinge, Keith Ditcham and Ardi Janjeva

RUSI Occasional Paper, January 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.

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

RUSI Occasional Paper, January 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 very grateful to Cifas for funding this project and being supportive partners throughout its duration. The authors would also like to thank all research participants who gave up their valuable time to contribute to this paper, including a number of individuals who provided helpful feedback on an earlier version, namely Martin Gill, Chris Greany and Marc Parker. We do not expect all of our views to be shared by those who have contributed to this research, but we are confident this is a better product thanks to their input.

This paper is written in memory of Major G G Brown (1925–2020) and in thanks for his support of Helena Wood's work at RUSI's Centre for Financial Crime and Security Studies.

Executive Summary

FRAUD AGAINST UK citizens, businesses and the UK public purse has reached epidemic levels – it is the 'volume crime of our time'.[1]

Driven in part by growing public disquiet over the current response to fraud, 2020 saw increased political attention on the issue. The prevailing political narrative, however, fails to convey the full impact of fraud on the UK, beyond the perspective of financial losses or the psychological impact on victims. Furthermore, continued under-resourcing of the fraud response means that political rhetoric fails to match operational reality. The fraud response is seen as continuing to fail the individuals, businesses and public bodies which fall victim to it with increasing regularity.

In order to inform a new approach to tackling fraud in the UK, this paper seeks to explore the broader social, economic and criminological impacts of fraud and their particular intersection with the UK national security landscape. In doing so, it sets out the case for adopting a fundamentally different pathway for responding to the problem.

First, the paper makes the case that when viewed in the context of the UK's National Security Objectives – particularly the objectives to 'protect our people' (National Security Objective 1) and 'promote our prosperity' (National Security Objective 3) – the limited consideration given to fraud in the national security dialogue seems increasingly perverse.

It is the crime to which UK citizens are most likely to fall victim,[2] and failures in the response to date have the capacity to undermine public confidence in the rule of law. Its impact on the private sector has consequences for both the stability of individual companies and the broader reputation of the UK as a place to do business. The scale of fraud against the public purse has been described as a 'heist on public services'[3] and has the capacity to undermine public faith and trust in government.

Given the wider social and economic damage caused, the case for placing fraud in the national security context should no longer be overlooked. On this basis, this paper makes the case for a new national security approach to tackling fraud, based on a 'whole of system' response, including

1. Cifas, 'Fraudscape 2019', p. 11, <https://www.cifas.org.uk/insight/reports-trends/fraudscape-2019>, accessed 18 December 2020.
2. The Office of National Statistics (ONS) Crime Survey for England and Wales noted 3.7 million incidents of fraud against individuals in the year ending March 2020. This outstrips 3.3 million theft offences against the person. See ONS, 'Crime in England and Wales: Year Ending March 2020', 17 July 2020, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2020#toc>, accessed 4 January 2021.
3. Author telephone interview with public official, August 2020.

a greater role for the government intelligence architecture, a better resourced and coordinated policing response and increased coordination with the private sector. In reframing this response, understanding fraud's interplay with more established national security threats, such as serious and organised crime (SOC) and terrorism, is also paramount. In the literature and government narrative to date, this relationship has been under-explored.

Second, therefore, this paper considers fraud as a vector of SOC. The very scale and nature of the most prevalent fraud typologies denote the involvement of organised crime groups, given either the sheer volume or the need for specialist skills to perpetrate the fraud. Despite this, there are considerable intelligence gaps surrounding fraud as an organised crime. This is particularly the case with regard to the threat emanating from overseas. This lack of understanding is found to be both a symptom and a cause of the under-representation of fraud in the SOC-specific operational response, particularly in policing – the lack of prioritisation being both symptomatic of the intelligence gaps and a cause of the limited intelligence picture needed to fill the gaps. To remedy this, the paper recommends more focused intelligence tasking from the National Security Council, a greater emphasis on fraud within the Strategic Policing Requirement and the breaking down of informational silos to make better use of cross-organisational data-matching tools.

Third, this paper explores fraud as a terrorist financing tool and finds ample examples of the 'repurposing' of well-established frauds to fulfil the financing needs of a wide range of terrorist actors. In this context, frauds against individuals – including courier fraud, online sales-based fraud and identity fraud – and the private sector echo many of the typologies seen in the organised crime sphere. On this basis, the paper makes the case for mandatory fraud investigation training for counterterrorism investigators as a key alternative disruption tool.

The role of fraud against the public sector is also explored, including benefit, tax credit and student loan fraud, and the key role these variants play in 'supporting the terrorist rather than the terrorist act'.[4] In assessing this, the paper makes the case for continuing the secondments of tax and benefits staff to the National Terrorist Financial Investigation Unit.

The wider social and economic impacts of fraud make a clear case for reframing the UK's fraud problem as a national security priority, for adopting a more centrally led, 'whole of system' response and for considerably augmenting the resources within the policing and intelligence community specifically assigned to tackling fraud. Furthermore, to ensure a better understanding of both the fraud threat and the way in which fraud acts as an enabler and vector of other threats, the rebuilding and reframing of the fraud response should not be carried out in isolation, but should build in organisational and informational links to the SOC- and terrorism-specific responses.

In summary, we should no longer be making the case for fraud as a national security concern – we should question the risk of not doing so.

4. Author video interview with former UK law enforcement officer, 1 July 2020.

Recommendations for Policymakers

Fraud: A National Security Response

Recommendation 1: The National Security Council (NSC) should commission a new 'whole of system', public–private strategy for tackling fraud. This should include: a new national to local networked criminal justice response; pathways for cross-government collaboration; and a clearer role for the private sector – including the financial, e-commerce and telecommunications sectors – in tackling fraud.

Recommendation 2: The 2021–26 National Cyber Security Strategy should establish a more explicit mandate for GCHQ in protecting the public from cyber fraud and should lay out a long-term resourcing plan for the National Cyber Security Centre Suspicious Email Service.

Recommendation 3: The National Police Chief's Council should commission a review to build synergies between the specialist fraud and cyber capabilities within policing, including exploring the benefits of functional mergers.

Recommendation 4: The 'Government Counter Fraud Profession' should be explicitly noted within National Security Objective 3 as part of critical government infrastructure and a means of protecting UK economic security and prosperity.

Recommendation 5: A new 'whole of system' public–private fraud strategy (see Recommendation 1) should specifically lay out an action plan for improving the enforcement response to frauds against businesses, using a range of criminal and civil tools.

Fraud as a Serious and Organised Crime

Recommendation 6: The NSC should issue a high-level intelligence requirement to the National Crime Agency (NCA) and the intelligence agencies to improve the national understanding of fraud as an organised crime. The NCA needs sufficient resourcing to achieve this.

Recommendation 7: The Strategic Policing Requirement should be amended to emphasise fraud as a serious and organised crime priority, led by the NCA, to ensure specialist resources are available for the investigation of serious and organised fraud.

Recommendation 8: A key goal of the National Economic Crime Centre's Public–Private Operational Board should be greater cross-dataset exploitation between fraud and serious and organised crime as a means of better understanding the threat from organised fraud.

Fraud as a Terrorist Financing Tool

Recommendation 9: The government should actively revisit the role that effective digital ID schemes can play in protecting against all forms of fraud, including as a tool for countering fraud for terrorist financing purposes, as part of its National Data Strategy.

Recommendation 10: Agencies charged with distributing benefits and government support should receive basic training on how to identify terrorist financing vulnerabilities and should make greater use of tech-based tools, such as IP address monitoring and geo-location tools, to ensure service users' locations are consistent with their supposed status.

Recommendation 11: Embedded positions for HMRC and Department of Work and Pensions staff in the National Terrorist Financial Investigation Unit should be maintained to help spot fraud disruption opportunities.

Recommendation 12: Emphasis should be placed on ensuring the necessary skills are maintained to ensure fraud investigation remains a key tool in the armoury of counterterrorism policing, with additional training on fraud investigation and prosecution provided where necessary.

Recommendation 13: The UK's Joint Money Laundering Intelligence Taskforce Terrorist Financing Working Group and the Joint Fraud Taskforce should establish a new cross-taskforce working group.

Introduction

'FRAUD, LIKE THE mythical Hydra of Ancient Greece, is a many-headed foe that is capable of disrupting society in a number of ways'.[1] This statement is certainly borne out in the UK, where the scale of fraud – a crime of deliberate deception for financial gain – against businesses, individuals and public finances continues to steadily increase.[2]

This manifests itself as year-on-year growth in the volume of fraud reported to the UK's three main fraud reporting bodies (Cifas, UK Finance and Action Fraud[3])[4] and has led industry experts to refer to fraud as the 'volume crime of our time'.[5] Fraud's impact is broad and reaches all areas of society, not least in economic terms; whilst the true cost of fraud may never be known, one report has put the aggregate fraud cost to the UK as high as £190 billion or 10% of UK GDP at that time.[6]

Despite historical neglect of fraud as a political, policy and policing priority, the past 12 months have seen a rapid increase in the amount of political airtime given to fraud, particularly at policy and parliamentary levels.[7] This is partly due to the publication of statutory reviews relating to failures in fraud policing,[8] high-profile exposés of fraud reporting services in the mainstream

1. Oliver Griffin, 'How Fraud Could Destabilise Global Economies', *Raconteur*, 11 September 2018.
2. A range of open source reporting indicators, such as the Annual Crime Survey for England and Wales, UK financial sector reporting (including UK Finance's annual 'Fraud: The Facts' reports), and Cifas' annual reports consistently show the steady growth of reported or detected fraud.
3. Cifas is a not-for-profit fraud prevention membership organisation managing a database of instances of fraudulent conduct in the country; UK Finance is the industry body representing UK financial institutions and collects data about fraud against its members; Action Fraud is the central police reporting service for fraud, run by the City of London Police.
4. Part of this growth may be accounted for by greater awareness of the reporting channels or better fraud detection processes. However, it was widely reported by interviewees in this research that detected and reported fraud only represents a small fraction of actual occurrence of fraud.
5. Cifas, 'Fraudscape 2019', p. 11, <https://www.cifas.org.uk/insight/reports-trends/fraudscape-2019>, accessed 18 December 2020. 'Volume crime' is defined by the National College of Policing as 'any crime which, through its sheer volume, has a significant impact on the community and the ability of the local police to tackle it'. See College of Policing, 'Volume Crime', <https://www.app.college.police.uk/app-content/investigations/introduction/#volume-crime>, accessed 5 October 2020.
6. 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.
7. See Parliamentlive.tv, 'Home Affairs Committee', 3 June 2020, <https://parliamentlive.tv/Event/Index/6f8da59b-0daf-473d-90f7-4dde9509dfc7>, accessed 29 October 2020.
8. HMICFRS, *Fraud: Time to Choose – An Inspection of the Police Response to Fraud* (London: The Stationery Office, 2019).

media[9] and, more recently, the emerging scale of frauds against the UK government's coronavirus pandemic business support schemes.[10]

Although the greater airtime for fraud in government, parliamentary and media circles is welcome, this has not resulted in the fundamental strategic shift in thinking needed to tackle the problem, with the debate continuing to view the issue primarily as one of criminal justice. While a policing and criminal justice response is clearly an essential part of the response (and one which this research found to be chronically under-resourced), this response alone has clear limitations against the modern face of fraud, which is increasingly cross-border and cyber enabled.

It is clear that without a major systemic shift in the UK government's strategic approach to tackling fraud, the issue will continue to fester unchecked. This paper starts with the premise that a new approach is needed. It examines the ways in which fraud has been under-represented as a national security risk to the UK, both as an issue in its own right and as a vector of established national security priorities, such as serious and organised crime (SOC) and terrorism. It then makes the case for a new and properly resourced 'whole of system' response, under the aegis of the UK's national security strategy, of which the criminal justice response is a core part, but not the whole.

Although fraud has been referenced (albeit in a limited way) in the UK's key national security documents since 2015, there has been limited exploration of fraud as a national security concern in its own right in the UK. The transformative effect of approaching key systemic concerns from a national security angle are clear from the way in which this has transformed the response in other areas, such as SOC or cyber security. These effects can broadly be articulated as:

- **Leadership**: Issues coming under a national security purview have traditionally benefited from a more centralised and coordinated response, both at a political and operational level.
- **Funding**: Threats given priority status under national security apparatus frequently fare better in spending reviews.
- **'Whole of system' response**: Establishing an issue as a national security concern ensures a clear responsibility for non-criminal justice departments, the diplomatic service and the wider intelligence architecture in tackling the issue.

In making the case for fraud as a national security concern for the UK, Chapter I examines the intersection of fraud with the UK's current national security objectives. Chapter II explores the evidence (and evidence gaps) surrounding some of the key perpetrators of fraud: serious and organised criminals. Chapter III examines an under-explored aspect of the fraud threat; namely

9. Paul Morgan-Bentley, 'Action Fraud Investigation: Victims Misled and Mocked as Police Fail to Investigate', *The Times*, 15 August 2019.
10. See, for example, Richard Walton, Sophia Falkner and Benjamin Barnard, *Daylight Robbery: Uncovering the True Cost of Public Sector Fraud in the Age of COVID-19* (London: Policy Exchange, 2020).

fraud as a terrorist financing tool. As a whole, these issues combined set out an irrefutable case for the necessity of accepting fraud as a threat to UK national security.

Methodology

This paper seeks to explore the research question: 'to what extent and in what ways does the UK's fraud threat intersect with its national security priorities and objectives?'.

Its findings are based on a review of publicly available literature, including UK government and law enforcement reporting, academic and third sector research, and journalistic material. Initial sources were identified by key word searches based on the research question with subsequent sources recommended by interview subjects.

This was supplemented by 27 semi-structured interviews conducted via telephone or video conferencing (due to the coronavirus pandemic) with leading UK-based fraud experts from the public, private and third sector as well as academics and experts in think tanks in the UK. The research team conducted 20 interviews between June and July 2020, with interviewees selected on the basis of either their public research profile or their position within the counter-fraud or national security architecture. Seven further interviews were conducted in August and September 2020, with interviewees who were identified based on the recommendations of initial expert interviews.

A qualitative approach was primarily adopted due to the limited amount of publicly available data.

Definitions and Scope

The two focus areas of this paper – fraud and national security – provide definitional challenges. Both are broad, umbrella terms encompassing numerous sub-categories, where no single agreed legal or conceptual definition exists.

To ensure manageability of research and to maintain a focused approach, the authors relied on the following conception of fraud. The research focused on categories of fraud which operate within the following working and legal definitions combined:

- **Working definition**: For the purposes of this research, the authors relied on the working definition that defines fraud as 'deliberate deceptions committed against another party in order to cause loss, primarily of a financial nature'. This is an amalgam of HMICFRS's definition of fraud as 'deceptions committed to make a financial gain'[11] and the Fraud Advisory Panel's definition of fraud as 'the deliberate use of deception or dishonesty to disadvantage or cause loss (usually financial) to another person or party'.[12]

11. HMICFRS, *Fraud: Time to Choose*.
12. Fraud Advisory Panel, 'An Introduction to Legislation', December 2015, <https://www.fraudadvisorypanel.org/wp-content/uploads/2015/12/Criminal-fraud-in-England-and-Wales-

- **Legal definition**: The scope of the research focuses on acts which are primarily prosecuted under sections 2, 3 and 4 of the Fraud Act 2006 (the common thread of which is dishonesty), rather than offences which would commonly be referred to as 'fraud' but which are primarily prosecuted under other acts, such as the Theft Act 1968 and 1978.

The legal definition often differs from the way in which the term is used at a working level (such as in journalism or by the public), where it is often used interchangeably with other financially motivated crimes, such as theft and corruption.[13]

The research team noted that the term 'fraud' is also often erroneously used interchangeably with 'white-collar crime'. This paper, however, notes a clear distinction between the high-volume and varying types of crimes which come under the broad legal and definitional banner of fraud and the narrower band of corporate criminality covered by the generally accepted definition of white-collar crime as given by Edwin Hardin Sutherland in 1949.[14] This paper focuses on the former, highlighting frauds perpetrated against individuals, businesses and the public sector, which account for the vast majority of fraud offending in the UK by volume, as distinct from the corporate offending captured by the more limited term 'white-collar crime'.

December2015.pdf>, accessed 18 December 2020.

13. Anton Moiseienko and Kayla Izenman, 'What's in a Name? Corruption and Fraud in the UK', *RUSI Occasional Papers* (June 2019).
14. Sutherland defined white-collar crime as 'a crime committed by a person of respectability and high social status in the course of their occupation'. See Edwin Hardin Sutherland, *White Collar Crime* (New York, NY: Dryden Press, 1949), p. 9.

I. Fraud and UK National Security Priorities: Identifying Intersections

THE GROWTH OF new technologies, while having widespread positive effects for the global economy, has offered unprecedented opportunities for the growth and globalisation of fraud as a volume crime. The UK is not alone in facing the challenges this presents, but certain factors collude to make it the perfect petri dish for its growth: it is an affluent country with a highly globalised financial sector and a ready pool of professional service providers, who wittingly or unwittingly enable fraud to be perpetrated at speed and scale.

However, these environmental factors alone do not explain why the UK has become a target destination for global fraudsters. Part of the blame lies at the door of the well-documented failures in the response needed to *deter* fraud. Over the past 15 years, a number of high-profile reviews in the UK – from the Attorney General's Fraud Review in 2006, to the HMICFRS review in 2019 and the Mackay Review in 2020 – have highlighted the paucity of resources allocated to tackling fraud.

Exacerbating the above factors is a systemic 'responsibility vacuum' in the UK government response to fraud, with ownership of the problem fragmented across different government departments and law enforcement and criminal justice agencies. With fraud continuing to be everybody's problem but nobody's priority, the UK has emerged as a low-risk/high-reward jurisdiction for fraudsters.

It is this paper's premise that many of the above issues could (and should) be remedied by adopting a more centralised and national security-driven 'whole of system' approach to tackling fraud, rather than the more limited criminal justice-centric approach adopted to date. As already mentioned, a national security approach has been seen to offer greater leadership, resources and the 'whole of system' approach necessary to tackle an endemic problem such as fraud.

In order to make an evidenced case for change, this chapter explores the ways in which fraud intersects with the UK's established national security objectives.

The UK's National Security Objectives

The UK adopted the following national security objectives in 2015, which remain in place at the time of writing:

- 'National Security Objective 1 is to **protect our people** – at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life'.
- 'National Security Objective 2 is to **project our global influence** – reducing the likelihood of threats materialising and affecting the UK, our interests, and those of our allies and partners'.
- 'National Security Objective 3 is to **promote our prosperity** – seizing opportunities, working innovatively and supporting UK industry'.[15]

Since the publication of the *National Security Strategy and Strategic Defence and Security Review*,[16] there has been increasing emphasis, at least at a rhetorical level, on economic crime as a growing threat to UK interests in its own right and one which 'makes other criminal activity easier'.[17] Given that the term 'economic crime' covers a broad suite of crimes,[18] it would be easy to surmise that fraud is already well covered in the UK's national security response. Indeed, fraud has frequently been mentioned in the slew of public-facing UK national security publications since 2015,[19] initially as a vector of SOC and latterly as a broadly defined economic crime threat.[20]

However, there has been a noticeable lack of focused exploration within the national security dialogue on the ways in which fraud, in its own right, intersects with the specific UK national security objectives. This is despite the rapidly evolving nature and scale of the fraud threat in the UK, which challenges the outdated notion of fraud as a crime solely against the vulnerable. The evidence put forward in this paper makes the case for fraud as a threat to UK citizens and critical financial infrastructure and a crime which threatens to destabilise public funding of essential services.

The ways in which these modern-day manifestations of the fraud threat intersect with National Security Objective (NSO) 1 and NSO 3 – deemed by the research team as the NSOs with the most explicit intersection with the UK's fraud threat – are explored below.

---

15. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, Cm 9161 (London: The Stationery Office, 2015), pp. 11–12.
16. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*.
17. HM Government, 'National Security Capability Review', March 2018, p. 23.
18. For a UK definition of economic crime, see HM Government and UK Finance, 'Economic Crime Plan: 2019–22', July 2019, p. 10.
19. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*.
20. HM Government, 'National Security Capability Review', p. 23.

Fraud and National Security Objective 1: Protecting Our People

The exact focus of NSO 1 – 'to protect our people' – is unclear other than a broad-based commitment to protect 'our territory, economic security, infrastructure and way of life'[21] against a range of disparate threats from hostile states, terrorism, cyber, SOC and natural disasters.[22] Specific to the field of fraud, however, the 2015 strategy commits to enhancing 'our ability to protect the public, businesses and the public sector from fraud and cyber-crime'.[23]

Despite this commitment, as noted by the University of Portsmouth's Centre for Counter Fraud Studies, 'the thin resources of the state dedicated to fighting fraud means that for most organisations and individuals the best they can do is protect themselves'.[24] The research for this paper confirmed that, at least from a criminal justice resourcing perspective, this remains true today.[25]

Fraud Against Individuals: The Silent Threat

According to data collected by the Crime Survey for England and Wales (CSEW),[26] there were 3.7 million incidents of fraud between March 2019 and March 2020.[27] This makes fraud the most likely crime that adults can fall victims to in the UK,[28] overtaking other crimes against personal property such as burglary, theft or robbery by a significant margin. For example, the CSEW noted only 356,000 incidents of burglary in the same period and 124,706 incidents of theft. While the 'hidden' nature of the crime makes assessing the true volume and cost of fraud against individuals difficult, it is clear from available statistics that the scale of the problem is vast,[29] with one report from 2017 suggesting that fraud against individuals was at that time as high as £6.8 billion.[30] The

21. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 23.
22. *Ibid.*, p. 11.
23. *Ibid.*, p. 42.
24. University of Portsmouth Centre for Counter Fraud Studies, 'Annual Fraud Indicator Report 2017', p. 5.
25. Various video interviews with serving public, private and third sector professionals, June–August 2020.
26. The annual survey of crime as experienced by UK households. Fraud was first included in this survey in 2015 following a request from the Home Office.
27. Office for National Statistics, 'Crime in England and Wales: Year Ending March 2020', Statistical Bulletin, July 2020, p. 26. These figures include both frauds reported to the police and frauds either not reported at all or those handled internally by banks.
28. Fraud overtook theft against the person as the most commonly experienced crime type in the Crime Survey for England and Wales in 2017. See Office for National Statistics, 'Crime in England and Wales: Year Ending June 2020', 28 October 2020, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2020>, accessed 5 January 2021.
29. These statistics include figures from Action Fraud, the UK's central portal for reporting fraud to the police. See City of London Police, 'Fraud Crime Trends 2019–20', <https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf>, accessed 3 December 2020.
30. University of Portsmouth Centre for Counter Fraud Studies, 'Annual Fraud Indicator Report 2017', p. 4. Research for this paper was unable to identify more up-to-date, reliable statistics covering the full scale

growing evidence of the scale of the issue, however, has not resulted in the levels of government funding or operational prioritisation deemed necessary to tackle the problem.[31]

The historical lack of political prioritisation of fraud may be strongly linked to the lack of salience accorded to it by the public. Polling suggests that the general public perceive fraud as a low-priority crime,[32] perhaps reflective of a generalised view of fraud as a crime solely committed against the more vulnerable, the elderly or (less generously) the naïve.[33]

Up-to-date public polling data is unavailable. However, interviews conducted for this paper with representatives from the public and private sectors suggest that attitudes to fraud may be changing as it begins to impact more citizens across a greater cross-section of ages and social strata.[34]

The authors' interviews and literature review point to the changing profile of fraud victims in the UK as a potential trigger for changing attitudes to fraud. Far from being a crime solely against the vulnerable, research for this paper indicates that fraudsters have evolved towards the use of sophisticated social engineering techniques[35] to target the UK population at random.[36] As noted by the Home Office in 2019, the 'typical' fraud victim is 'more likely to be in higher income households, in managerial/professional occupations and aged 25-54, challenging the common belief that fraud is solely a problem amongst the elderly'.[37] In short, the shift from fraud as a crime

---

of fraud against individuals.

31. The Spending Review 2020 allocated a £20-million capital spend for the central reporting body Action Fraud, but did not include funding for wider policing reform or investment in intelligence capabilities. See HM Treasury, *Spending Review 2020*, CP 330 (London: The Stationery Office, 2020).
32. In a recent report commissioned by HMICFRS, only 5% of respondents noted 'fraud' as a priority against 49% for terrorism, 38% for organised crime and 18% for burglary and theft offences. See BMG Research, 'Public Perceptions of Policing in England and Wales 2018', January 2019.
33. Author video interview with academic researcher in fraud, July 2020. Research by the 'Take Five to Stop Fraud' campaign in 2017 also noted that 80% of people thought they could confidently identify a fraudulent approach. See Take Five to Stop Fraud, 'Consumers Think They Are Too Smart to be Scammed', 22 January 2017, <https://takefive-stopfraud.org.uk/news/consumers-think-too-smart-scammed/>, accessed 19 August 2020.
34. Author interviews with eight public and private sector counter-fraud professionals, July and August 2020.
35. Social engineering is a method in which criminals manipulate people into either transferring money or divulging their personal details, often by posing as a legitimate business or law enforcement official. See Nate Lord, 'What is Social Engineering? Defining and Avoiding Common Social Engineering Threats', *Data Insider* (Digital Guardian blog), 11 September 2018, <https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats>, accessed 29 October 2020.
36. Maria Keyworth, 'Vishing and Smishing: The Rise of Social Engineering Fraud', *BBC News*, 1 January 2016.
37. Home Office, *The Scale and Nature of Fraud: A Review of the Evidence* (London: Home Office, July 2018).

against the vulnerable to fraud as an indiscriminate crime may, in part, be influencing a growth in political attention.

Box 1: Growth of Authorised Push Payment Fraud

The shift towards social engineering techniques is particularly evident in the field of payment system and card fraud; the fraud type most reported to Action Fraud by volume in the UK in 2019/20.[*] Measures introduced over the past 15 years, from 'chip and pin' technology to the recent introduction of the 'confirmation of payee' scheme in 2020,[†] have reduced the opportunity for 'unauthorised' card and payment fraud,[‡] which, according to UK Finance, has been falling year on year.[§] According to interviews with financial sector fraud experts,[‖] this has forced criminals to shift their focus from manipulating banking systems to manipulating individuals into making the payment themselves. These types of frauds, known as 'authorised push payment frauds' (APP),[¶] have seen a rapid growth over the past five years. According to UK Finance, reporting of APP frauds saw a 29% increase in 2019, causing a loss of £456 million to customers.[**]

Whereas 'unauthorised' payment frauds are often seen as 'victimless' crimes and a banking system's problem (as the legal duty, by and large, falls on banks to repay the victim), the growth of more sophisticated APP frauds has a two-fold impact on the victim. The direct manipulation of the victim has a more damaging psychological impact and the complicity of the victim in the payment (albeit innocent) means they are not automatically entitled to compensation from the bank.

[*] Action Fraud is the UK's central fraud reporting hub. Statistics taken from Action Fraud's 2019–20 crime trends data notes 381,572 reports of 'cheque, plastic card and bank account fraud' reported to Action Fraud, Cifas and UK Finance collectively in that period, making it the most reported fraud type by volume. See Action Fraud, 'Fraud and Cyber Crime National Statistics', 6 October 2020, <www.actionfraud.police.uk/data>, accessed 5 January 2021.

[†] See pay.uk, 'Confirmation of Payee', <https://www.wearepay.uk/confirmation-of-payee/>, accessed 6 October 2020.

[‡] An unauthorised fraudulent transaction is when the account holder does not provide authorisation for the payment and the payment is instigated by a third (criminal) party.

[§] See UK Finance's annual 'Fraud – The Facts' reports at <https://www.ukfinance.org.uk/>, accessed 19 August 2020.

[‖] Author video interview with financial sector fraud experts, July 2020.

[¶] In an authorised push payment fraud, the genuine customer is tricked, often using sophisticated social engineering techniques, into making the payment themselves to another account which is controlled by a criminal.

[**] UK Finance, 'Fraud – The Facts 2020: The Definitive Overview of Payment Industry Fraud', March 2020, p. 5.

Despite the growing scale of the problem and the changing victim profile, the operational response has not kept pace: there is no national cross-government strategy for tackling fraud; fraud only represents 1% of the policing response;[38] and while vulnerable victims get a largely good response, the vast majority of victims do not.[39]

This paper therefore makes the case for adopting a new cross-government strategy, under the leadership of the National Security Secretariat,[40] which sets out a single guiding mission and action plan for the UK's counter-fraud effort, both public and private, and clear reporting and accountability lines.

As regards the public sector response, this strategy should set out a resourcing model for the criminal justice response, with a significant resource uplift to fill the substantial capacity gap. This should be accompanied by root-and-branch structural reforms, including the adoption of a centrally networked policing response, akin to the structure adopted in counterterrorism policing, with officers placed at the national, regional and local policing tiers, but aligned to existing policing structures. It should also set out the importance of cross-departmental information sharing and operational collaboration. Furthermore, the strategy should set out a clearer role for the intelligence services in the UK's counter-fraud response.

Given the frontline role played by the private sector in identifying and preventing fraud, the strategy should be a public–private response, in particular reflecting the important roles and responsibilities of particular strata of the private sector in tackling fraud, such as the financial sector, e-commerce, social media and telecommunications industries.

Recommendation 1: The National Security Council (NSC) should commission a new 'whole of system', public–private strategy for tackling fraud. This should include: a new national to local networked criminal justice response; pathways for cross-government collaboration; and a clearer role for the private sector – including the financial, e-commerce and telecommunications sectors – in tackling fraud.

38. Graeme Biggar, Director General of the National Economic Crime Centre, gives evidence to the Home Affairs Select Committee inquiry into online crime, 3 June 2020, <https://www.parliamentlive.tv/Event/Index/6f8da59b-0daf-473d-90f7-4dde9509dfc7>, accessed 5 January 2021.
39. HMICFRS, *Fraud: Time to Choose*, p. 7.
40. The National Security Secretariat is the government body responsible for coordinating the national security response.

The Fraud–Cyber Interface: A Marriage of Convenience

The increasing digitalisation of everyday life has brought with it an array of cyber threats to the UK. In recognition of the scale of the threat, 'cyber' now has 'Tier 1' national security status,[41] prominence under NSO 1 and a bespoke cross-government 'National Cyber Security Strategy'.[42]

However, despite fraud having reasonable prominence within the cyber threat rhetoric, interviews noted that, in practice, fraud receives less prominence in terms of the operational cyber-specific response.[43] This is despite figures from Action Fraud, the central UK law enforcement fraud reporting channel, showing that 85% of reported fraud in 2019/20 was cyber enabled (referred to hereafter as cyber fraud).[44] The growth of fraud as a cyber threat facing the UK may not have been altogether clear when the National Cyber Security Strategy was published in 2016,[45] but now it seems incontrovertible.

Particularly with regard to volume fraud, it is clear that the vast majority of this is at least cyber assisted. Based on interviews for this paper, as well as recent contributions to the literature,[46] it is apparent that there is an increasing drive for policymakers to embrace these overlaps and ensure that specialists across cyber, fraud and financial crime are connected. Despite the increase in policy coordination, we are yet to see this translate into a necessary cross-disciplinary operational response. The current operational response to fraud continues to be delivered largely through a traditional criminal justice response, led by local policing teams with a specific geographic remit. The current policing response, which is culturally inclined towards a physical (rather than virtual) investigation model, is ill-suited to dealing with most cyber frauds, where perpetrators and individual victims are rarely confined to one force area or even one country. This means many cross-border frauds are not investigated.

Furthermore, the low-value/high-volume nature of many cyber frauds means they struggle for operational priority under the Management of Risk in Law Enforcement (MoRILE) scoring system[47] used by most local forces to prioritise investigations, given the losses to individual

41. See GCHQ, 'The Cyber Threat', 11 April 2016, <https://www.gchq.gov.uk/information/cyber-threat>, accessed 6 October 2020.
42. HM Government, 'National Cyber Security Strategy 2016–2021', November 2016.
43. Based on four author video interviews with fraud law enforcement professionals, August 2020.
44. City of London Police, 'Fraud Crime Trends 2019–20'.
45. HM Government, 'National Cyber Security Strategy 2016–2021'.
46. Sneha Dawda, Ardi Janjeva and Anton Moiseienko, 'Rethinking the UK Response to Cyber Fraud: Key Policy Challenges', RUSI Briefing Paper, July 2020; UK Finance, 'Staying Ahead of Cyber Crime', April 2018; 41st Parameter, 'Surveillance, Staging and the Fraud Lifecycle: Turning the Tables on Cyber Criminals', 2014; David S Wall, 'How Big Data Feeds Big Crime', *Current History* (January 2018), pp. 29–34.
47. MoRILE is the operational prioritisation system used in policing to assess case adoption. The system assesses (among other things) the impact, physical, psychological and financial harm to

victims in local force areas may be low when taken in isolation. On this basis, there is a clear case for a more disruption-based approach to tackling cyber fraud in the longer term.

Recognition of the role of disruption was evident in the launch of the National Cyber Security Centre's (NCSC) Suspicious Email Reporting Service (SERS) in April 2020, a mechanism for the public to report potential 'phishing' emails,[48] which by 30 November 2020 had taken down 45,582 URLs linked to 22,192 scams.[49] This is a welcome move, but the long-term role and resourcing of the SERS function is not clear. The growing scale of 'fraud as a cyber-enabled crime' gives cause for a more considered role for the UK's cyber intelligence machinery in tackling the issue.

Recommendation 2: The 2021–26 National Cyber Security Strategy should establish a more explicit mandate for GCHQ in protecting the public from cyber fraud and should lay out a long-term resourcing plan for the NCSC's SERS.

That said, while disruption-based approaches have a clear role in tackling cyber fraud, this does not negate the need for greater use of mainstream criminal justice outcomes, such as prosecutions and asset recovery, as part of an overall approach to raise the risk and reduce the rewards of committing cyber fraud.

Research interviews suggest that the continued delineation within policing (both functional and budgetary) between 'fraud' and 'cyber' policing roles undermines the ability to build a multi-functional approach to tackling the issue.[50] This has led to growing calls from senior police officers to break down the increasingly arbitrary delineation between fraud and cyber policing[51] and the recent appointment by the National Police Chief's Council of a joint fraud and cyber response lead, housed at City of London Police.[52] It is not yet clear what tangible outcome this role change may achieve. So far, this has yet to translate into changes at the operational level.

---

individuals, which in individual cyber-enabled fraud cases may be low despite a high aggregate harm level of frauds committed as a volume crime by an individual crime group.

48. Phishing is the sending of emails to innocent parties, frequently posing as legitimate companies or government agencies in order to induce them to reveal personal data with the aim of using that data for fraudulent purposes.
49. National Cyber Security Centre, 'Phishing: How to Report to the NCSC', 21 April 2020, <https://www.ncsc.gov.uk/information/report-suspicious-emails>, accessed 4 December 2020.
50. Four author video interviews with fraud law enforcement professionals, August 2020.
51. Karen Baxter, Head of Economic Crime, City of London Police, gives evidence to the Home Affairs Select Committee inquiry into online crime, 3 June 2020, <https://www.parliamentlive.tv/ Event/ Index/6f8da59b-0daf-473d-90f7-4dde9509dfc7>, accessed 5 January 2021.
52. Author video interview with senior officials, September 2020.

Recommendation 3: The National Police Chief's Council should commission a review to build synergies between the specialist fraud and cyber capabilities within policing, including exploring the benefits of functional mergers.

To summarise the above, to establish a national security objective 'to protect our people' without consideration of the crime of which they are most likely to fall victim appears increasingly perverse.

Fraud and National Security Objective 3: Promoting Our Prosperity

An expanded definition of national security in the post-Cold War landscape has led to the greater prominence of economic security as a facet of national security at national and global levels.[53] This new national security paradigm has been fully adopted in the UK, as evidenced by the National Security Capability Review 2018 noting that 'economic security is a core part of the UK's national security agenda'.[54]

Within NSO 3, the symbiotic nature of the relationship between national security and economic security is laid bare – a strong economy allows for investment in national security, and investment in national security provides for a stable business and investment environment which drives prosperity.[55]

Although estimating the true scale of the fraud cost to the UK economy is widely accepted as a highly challenging task,[56] some estimates range from £130 billion[57] to £190 billion[58] per annum. Whatever the true cost, it is clear that fraud, if left unchecked, has the potential to destabilise UK economic security and prosperity.

Despite this, fraud's relevance to NSO 3 has been under-emphasised in the national security dialogue to date. This paper therefore sets out the ways in which fraud presents a threat to UK national prosperity by looking at the issue from two angles:

- The economic impact of fraud against the public sector.
- The impact of fraud on the UK as a place to do business.

53. See, for example, Lucia Retter et al., 'Relationships Between the Economy and National Security', RAND Europe, 2020.
54. HM Government, 'National Security Capability Review 2018', p. 36.
55. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 70.
56. Outcome of a RUSI–Home Office workshop with approximately 30 UK academics, February 2020.
57. Jim Gee and Mark Button, 'The Financial Cost of Fraud 2019: The Latest Data from Around the World', Crowe and University of Portsmouth, 2019, p. 6.
58. University of Portsmouth Centre for Counter Fraud Studies, 'Annual Fraud Indicator Report 2017', p. 3.

The Economic Impact of Fraud Against the Public Sector

The UK National Security Strategy highlights that a strong national security response requires substantial government investment, predicated on well-managed public finances.[59] However, despite significant advances in tackling public sector fraud since the establishment of the Government Counter Fraud Function in 2018,[60] public bodies in the UK are estimated to lose between 0.5% and 5% of their spending to fraud – or between £31 billion and £48 billion per annum.[61] In context, the upper end of this range roughly equates to the UK's annual defence budget of £41.5 billion for 2020/21.[62]

This figure contains the full gamut of frauds against the public purse, from low-level frauds perpetrated by individuals to organised frauds against the Exchequer. Whilst these cannot individually be said to represent a national security threat, research for this paper demonstrates that the collective scale of the problem amounts to what can be described as a 'heist on public services',[63] given that every pound lost to fraud is a pound which cannot be spent on frontline services.

Understanding of the specific nature of the fraud threat against the public sector remains patchy, particularly in terms of perpetrators' profiles. It is therefore essential that work to better understand the nature of the threat is prioritised by intelligence agencies as a means of furthering the response. Working to reduce this figure even by a small percentage will be an essential means of protecting the UK's economic security in the future.

Despite the substantial loss to the public purse involved, the rationale for investing in public sector counter-fraud goes beyond simply the financial impact; it is important to recognise the impact that unfettered fraud against the public sector can have on the relationship between the state and its citizens. As noted by the International Public Sector Fraud Forum (IPSFF):

> Significant fraud against a public body may result in general erosion of trust in government. This can negatively impact how people conduct business at personal, industry and state levels … Erosion of trust in the integrity of the public sector has been shown to lead to a decrease in legal compliance.[64]

---

59. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015*, p. 6.
60. See HM Government, 'Counter-Fraud Standards and Profession', <https://www.gov.uk/government/groups/counter-fraud-standards-and-profession>, accessed 24 August 2020.
61. International Public Sector Fraud Forum, 'Guide to Understanding the Total Impact of Fraud', February 2020, p. 26. Note that this figure is likely to be substantially higher once the scale of individual and organised frauds against coronavirus-related business support schemes are fully accounted for.
62. Ministry of Defence, 'UK Defence in Numbers: 2019', February 2020, p. 1.
63. Author video interview with public sector official, September 2020.
64. See International Public Sector Fraud Forum, 'Guide to Understanding the Total Impact of Fraud', p. 15.

This could well extend to a societally pervasive culture in which low-level fraud against the public purse is accepted, with fraud emerging, in Susanne Karstedt and Stephen Farrall's words, as a 'crime of everyday life'.[65]

On this basis, protecting – and growing – the government's nascent counter-fraud profession should be viewed not just as good practice in and of itself, but also as a key means of protecting the UK's economic security, securing public faith in government and by extension protecting UK national security. Despite the clear benefits of investment in this area, however, the funding model for growing this function remains unclear.[66]

Recommendation 4: The 'Government Counter Fraud Profession' should be explicitly noted within NSO 3 as part of critical government infrastructure and a means of protecting UK economic security and prosperity.

The Impact of Fraud on the UK as a Place to Do Business

By value, the private sector is by far the biggest victim of fraud in the UK. Although an under-researched area, one estimate from 2017 put the cost of fraud against the private sector at £140 billion.[67]

Whatever the true figure, the financial implication of fraud against businesses is self-evident in the way in which fraud is dealt with in accounting terms – as a 'cost' on the balance sheet. At best, fraud losses cause a short-term hit to reputation and reduce working capital available for investment. At worst, these losses can threaten the financial viability of a company.[68]

Far from just harming individual businesses, however, if left unchecked, fraud against the private sector has the potential for longer-term macro-economic impact on UK prosperity. First, as a 'cost' to business, fraud reduces business profits, thus reducing the amounts payable to the Exchequer in tax. Second, as the UK seeks to establish a more independent profile on the international stage post-Brexit, an unfettered business fraud problem has potential impact on the reputation of the UK as a destination for investment. As noted by the IPSFF, 'fraud can impact the international and economic reputation of countries. Widespread fraud can be a contributing factor in assessments of whether a country is safe to conduct international trade and business'.[69]

65. Susanne Karstedt and Stephen Farrall, 'The Moral Economy of Everyday Crime', *British Journal of Criminology* (Vol. 46, No. 6, November 2006), pp. 1011–36.
66. See RUSI, 'Economic Crime Plan Tracker', Action 29 Narrative, <https://www.rusi.institute/ecp/>, accessed 28 August 2020.
67. University of Portsmouth Centre for Counter Fraud Studies, 'Annual Fraud Indicator Report 2017', p. 10. This figure includes both losses and investigation costs.
68. Josie Cox, 'Half of UK Companies Have Been Victims of Fraud or Economic Crime in Last Two Years, PwC Study Shows', *The Independent*, 21 February 2018.
69. International Public Sector Fraud Forum, 'Guide to Understanding the Total Impact of Fraud', p. 15.

Nowhere is this issue of greater salience than in the case of the UK's financial sector, which is simultaneously a key pillar of the UK economy and the sector most vulnerable to fraud. According to UK Finance, the UK's financial sector trade body, criminals successfully stole £1.2 billion[70] through the payments industry in 2019, with wider estimates of financial sector fraud losses amounting to £5.2 billion.[71] The importance of tackling financial sector fraud was demonstrated by the think tank Policy Exchange in 2020, which noted that 'fraud impacts the integrity and reputation of the UK's financial services sector, which will play a vital role in the success of Britain after its withdrawal from the European Union (EU)'.[72]

Despite reported improvements in public–private cooperation to tackle financial sector fraud, particularly since the establishment of the National Economic Crime Centre (NECC) in 2018, the predominant focus of efforts remains on *prevention* of financial sector fraud, rather than *pursuit* of those perpetrating the crime.[73] This continues to mean that fraudsters view fraud against the UK financial sector as a low-risk/high-reward environment.

Table 1: Financial Sector Frauds: Trajectory Over Time

Year	Unauthorised Fraud (£ millions)	Authorised Push Payment Fraud (£ millions)	Total (£ millions)
2017	732	236	968
2018	849	354	1,203
2019	825	456	1,281

Source: UK Finance, 'Fraud – The Facts' reports (2018, 2019, 2020).

Despite the scale, reach and impact of fraud against the private sector, it receives no prominence in the national security dialogue in relation to the UK's prosperity agenda. Furthermore, interviews conducted for this paper suggest that the policing response to fraud against businesses is even less satisfactory than the response to fraud against individuals,[74] leading to a growth in private prosecutions by corporate victims when faced with an underwhelming police response.[75]

As the UK recovers from the financial impact of the coronavirus pandemic and prepares for life in a post-Brexit business environment, the government's inadequate response to fraud against

70. UK Finance, 'Fraud – The Facts 2020', p. 4.
71. University of Portsmouth Centre for Counter Fraud Studies, 'Annual Fraud Indicator Report 2017', p. 14.
72. Walton, Falkner and Barnard, *Daylight Robbery*, p. 11.
73. Author interviews with financial sector professionals, July and August 2020.
74. *Ibid.*
75. See, for example, 2 Hare Court, 'Increasing Regulation of Private Prosecutions', 8 October 2019, <https://www.2harecourt.com/training-and-knowledge/increasing-regulation-of-private-prosecutions/>, accessed 6 October 2020.

the private sector, typified by the lack of acknowledgement of the wider impacts of fraud on UK prosperity, has the potential to undermine both the UK's immediate financial recovery and its future position in the global economy.

For this reason, it is important that a 'whole of system' strategy is public–private in nature and includes a specific action plan for improving the enforcement response to fraud against the private sector.

Recommendation 5: A new 'whole of system' public–private fraud strategy should specifically lay out an action plan for improving the enforcement response to frauds against businesses, using a range of criminal and civil tools.

In sum, to prioritise UK economic security and prosperity, without due consideration of the extent to which the UK's fraud problem challenges both public and private financial stability and tarnishes the UK's attractiveness as a place to do business, would appear to be short-sighted.

II. The Fraud–Organised Crime Nexus

SERIOUS AND ORGANISED crime (SOC) has been described as 'the most deadly national security threat faced by the UK'.[76] It is said to affect more UK citizens, more often, than any other national security threat, and also impacts public services, businesses, institutions, national reputation and infrastructure.[77]

'SOC', however, is a broad umbrella term covering a multitude of wrongdoings; the main unifying motivation of which, in most cases,[78] is profit. In this way, fraud represents an appealing opportunity to organised crime groups (OCGs) attracted to its low-risk/high-reward nature.

Indeed, the idea of fraud as an organised crime is not novel; some frauds, by their very nature, require a level of specialism and organisation, as this chapter demonstrates, that is inherent in the very definition of an OCG.[79] Despite this, research for this paper found that fraud receives less prominent billing in the national security discourse surrounding SOC and minimal prioritisation within the SOC-specific operational response.[80]

Therefore, in addition to examining fraud as a national security threat (see Chapter I), exploring the role of organised crime within the fraud landscape will be key to understanding the extent to which fraud is amplifying the harm caused to the state and its citizens from organised crime and – therefore – impacting UK national security.

Organised Fraud: A Knowledge Gap

As noted, one reason for the limited prioritisation of fraud as a SOC threat is the dearth of intelligence and independent research relating to both the nature and scale of frauds perpetrated by organised criminals. Whereas it is commonly accepted that volume frauds, particularly cyber frauds, require some level of group organisation, there is limited understanding about the specific

76. HM Government, *Serious and Organised Crime Strategy*, Cm 9718 (London: The Stationery Office, 2018), p. 3.
77. National Crime Agency (NCA), 'National Strategic Assessment of Serious and Organised Crime', 2020.
78. The exception to this is organised child sexual exploitation, which is often driven by other motives.
79. The Serious Crime Act 2015 defines an 'organised crime group' as a group that has 'as its purpose, or as one of its purposes, the carrying on of criminal activities, and consists of three or more persons who act, or agree to act, together to further that purpose'.
80. Author telephone and video interviews with law enforcement professionals (current and former), June–August 2020.

form these networks take, the extent of poly-criminality (groups who shift between different types of criminality)[81] and the non-financial harms associated with this form of organised crime.

Gaps exist in relation to law enforcement's understanding of fraud as an organised crime. Interviews suggest that in other areas of the SOC threat, such as drug trafficking, law enforcement investment has resulted in a more holistic understanding of the criminal networks involved. On the other hand, the largely reactive nature of the fraud response[82] has resulted in a limited understanding of the organised fraud threat and in turn a lack of operational prioritisation of fraud within SOC resourcing, leading some respondents to label fraud the 'Cinderella of crime'.[83]

Part of the way in which this manifests itself is in the gaps surrounding the mapping of organised fraud groups in the UK. The UK's Organised Crime Group Mapping (OCGM) is one of the main tools used by UK law enforcement to prioritise operations and regulate access to the specialist tools available to tackle organised crime.[84] As noted by HMICFRS, however:

> At the end of 2017, there were 842 organised crime groups mapped in the United Kingdom that were believed to be involved in fraud. We found, however, that organised crime groups whose *primary* offence was fraud were generally not being mapped. Investigators told us that crime groups involved in firearms and drugs offences were more likely to be identified and mapped than fraudsters.[85]

The HMICFRS report found that only one police force routinely mapped OCGs whose primary offending was fraud. Not only does this lack of fraud mapping lead to a skewed picture of organised crime in the UK, it also limits the prioritisation of fraud as an organised crime threat when bidding for specialist tools and resources.

Further gaps exist around the specific nature of the international threat from fraud and the interplay between OCGs' fraud activities and their other SOC activities.

Despite well-documented instances of volume frauds being perpetrated by highly organised overseas-based crime groups, specifically targeting the UK,[86] the strategic understanding of the scale of the international organised fraud threat remains scant, with one senior fraud professional interviewed during this research commenting that, despite 30 years of investigating fraud, they still had no idea what proportion of the threat emanates from overseas.[87] Another

81. Adapted from NCA, 'National Strategic Assessment of Serious and Organised Crime', 2019, p. 4.
82. Author interview with academic researcher, July 2020.
83. Author interview with policy official, October 2020.
84. For more information, see College of Policing, 'Threat, Risk and Harm: Scoring of OCGs (Organised Crime Groups)', <https://whatworks.college.police.uk/Research/Research-Map/Pages/ResearchProject.aspx?projectid=709>, accessed 7 October 2020.
85. HMICFRS, *Fraud: Time to Choose*, p. 18. Emphasis added.
86. Rajini Vaidyanathan, 'Confessions of a Call-Centre Scammer', *BBC News*, 8 March 2020.
87. Author interview with senior fraud professional, August 2020.

interviewee explained how the lack of priority afforded to fraud is largely attributed to a lack of understanding of the global context of the international criminality behind it.[88]

This deficiency of knowledge extends to the limited understanding of the links between fraud and other forms of SOC. Research by Michael Levi notes that two-thirds of OCGs whose primary activity is fraud are also involved in other criminal activities.[89] Since the publication of Levi's research in 2014, examples of poly-criminality – including a case where significant earnings from postal scams were allegedly used to purchase firearms and ammunition sold to other OCGs[90] – have highlighted the potential overlaps. Overall, however, the collective knowledge on the extent of poly-criminality continues to be poor.

Despite the considerable knowledge and intelligence gaps in this area, where statistics do exist they challenge the portrayal of fraud as a lower-harm crime perpetrated by opportunistic criminals. Instead, they point to fraud as part of a bigger portfolio of illegal money-making ventures committed by career criminals.[91] For example, ground-breaking research by Tiggey May and Bina Bhardwa in 2017 found that 'OCGs involved in fraud are considered to have intent and capability across a wider range of areas, including expertise in infiltration, corruption and subversion, as well as involvement in multiple enterprises, good resistance and/or resilience tactics, and access to a ready cash flow'.[92]

By its very nature, it is challenging to pinpoint what percentage of fraud is perpetrated by OCGs. However, Police Foundation research from 2017 found that between 31% and 45% of fraud investigated by local police forces was linked to OCGs.[93] This figure fluctuates depending on victim location and the type of fraud, with perpetrators of rogue trading or doorstep fraud more likely to be local and acting alone or in very small numbers.[94] Additionally, law enforcement officers interviewed as part of May and Bhardwa's research estimated that 'the majority, or as much as 90%, of the fraud cases they investigated were committed by OCGs'.[95] While the real figure will never be known, these estimates point to a notable proportion.

In summary, despite being the most common crime type affecting individuals in the UK, the understanding of fraud as a vector of the organised crime threat continues to be poor, both

88. Author interview with law enforcement agency, August 2020.
89. Michael Levi, 'Organized Fraud', in Letizia Paoli (ed.), *The Oxford Handbook of Organized Crime* (Oxford: Oxford University Press, 2014), p. 462.
90. Author interview with law enforcement agency, August 2020.
91. Simon Avery, 'For Fraud, Look Under "Serious and Organized Crime"', *Public Money and Management* (Vol. 20, No. 5, 2020), p. 411.
92. Tiggey May and Bina Bhardwa, *Organised Crime Groups Involved in Fraud* (London: Palgrave Macmillan, 2018), p. 23.
93. Ruth Crocker et al., 'The Impact of Organised Crime in Local Communities', Police Foundation, June 2017, p. 62.
94. *Ibid.*, p. 56.
95. May and Bhardwa, *Organised Crime Groups Involved in Fraud*, p. 61.

in terms of the nature of the networks and scale of the problem. This lack of understanding of the issue partly explains the lack of prioritisation of fraud as a SOC threat. The intelligence gaps in this area should be a concern for policymakers, law enforcement and security officials, particularly as the world enters an accelerated phase in the digitalisation of social life.

Recommendation 6: The NSC should issue a high-level intelligence requirement to the NCA and the intelligence agencies to improve the national understanding of fraud as an organised crime. The NCA needs sufficient resourcing to achieve this.

Organised Crime: An Augmenter of the Fraud Threat

Although the full strategic picture of 'fraud as an organised crime' remains patchy, there are clear instances where the scale or complexity of certain fraud types automatically put them into the realm of organised crime.[96] This paper broadly delineates these fraud typologies along two lines:

- **Professionally organised frauds** where the involvement of OCGs with their inherent access to criminal skills and resources allows them to perpetrate the fraud in a rapid and scalable manner.
- **Professionally enabled frauds** that necessitate the use of specialist services and professional enablers[97] from outside the OCG to give the illusion of a legitimate business to facilitate the fraud.

The next section expands on these definitions and illustrates the specific methodologies involved using case studies.

Professionally Organised Fraud

OCGs are often comprised of individuals that have finely honed skillsets and experience in conducting certain types of crime, augmented by networks that facilitate access to markets where a good or service is in demand.[98] Where there is a gap in the skillset needed to commit a crime, OCGs are likely to have the means to source individuals who can fill that gap on a temporary basis.[99]

96. Levi, 'Organized Fraud'.
97. 'Professional enablers' can be defined as lawyers, accountants and other professions with skills which may support the commission of criminality.
98. Rick Brown and Russell G Smith, 'Exploring the Relationship Between Organised Crime and Volume Crime', Australian Institute of Criminology, *Trends and Issues in Criminal Justice* (No. 565, December 2018), p. 6.
99. *Ibid.*, p. 8.

This level of professional organisation means that whilst certain frauds are not technically advanced and *could* be perpetrated by lone actors, OCGs are better placed to commit certain types of fraud at an industrial scale and speed.

Case Study: Coronavirus Frauds

It is known that OCGs are among the most resilient adversaries the UK faces, quick to exploit opportunities on a transnational scale.[100] This was shown to be particularly true in how quickly fraudsters adapted to the opportunities presented by the coronavirus pandemic.

Law enforcement noted a sharp increase in the reporting of scams[101] targeting individuals and businesses, including 'click here for a cure' emails,[102] the fake offer of a coronavirus tax refund purportedly from the UK government[103] and others claiming they represent the World Health Organization with 'donate here to help the fight' appeals.[104] All share a common goal to defraud individuals and/or organisations and state entities, reaching potential victims across the globe through the internet. As noted by a law enforcement interviewee, 'the first reaction to the PPE [personal protective equipment] crisis was that organised crime had inserted themselves [sic] into that network; a network of capabilities which can mobilise itself very quickly especially in times of crisis and which can jeopardise areas of key national interest'.[105]

Furthermore, the state itself was not immune to targeting by organised fraudsters. Early evidence from media investigations[106] and the National Audit Office (NAO)[107] suggests that organised criminals moved quickly to target the variety of government-backed business support schemes. The high vulnerability of these schemes to organised crime exploitation stemmed from the fact that, as noted by the NAO:

> Once government decided to support small businesses facing cash flow problems owing to the pandemic, it moved very quickly to set up a scheme. It prioritised one aspect of value for money – payment speed – over almost all others and has been prepared to tolerate a potentially very high level of losses as a

100. HM Government, *Serious and Organised Crime Strategy*, p. 3.
101. See NCA, 'Beware Fraud and Scams During Covid-19 Pandemic Fraud', 26 March 2020, <https://nationalcrimeagency.gov.uk/news/fraud-scams-covid19>, accessed 7 October 2020.
102. Joe Tidy, 'Coronavirus: How Hackers are Preying on Fears of Covid-19', *BBC News*, 13 March 2020.
103. Leke Oso Alabi, 'Taxpayers Targeted by HMRC Coronavirus Scam', *Financial Times*, 11 March 2020.
104. Ardi Janjeva, 'The Coronavirus Pandemic Demands Digital Vigilance, Amid Intensifying Social Isolation', *RUSI Commentary*, 1 April 2020.
105. Author interview with law enforcement professional, August 2020.
106. Angus Crawford, 'Coronavirus: "My Name Was Used to Steal a Government Covid Loan"', *BBC News*, 28 September 2020.
107. National Audit Office (NAO), 'Investigation into the Bounce Back Loan Scheme', HC 860, 7 October 2020.

result. These losses can stem from businesses wanting to pay back loans but finding themselves unable to, through to organised criminals taking out loans with no intention of ever paying them back.[108]

Although the full scale of the impact of organised crime on UK coronavirus support schemes is yet to be revealed, one high-profile incident was revealed in the North Rhine–Westphalia region of Germany. Here, the state government paid out over €2.3 billion in a day as part of its economic recovery strategy but had to pause its activity within a week after it was found that more than 90 fake websites had been scraping masses of data from companies applying for emergency grants and diverting money into criminal hands.[109]

As stated by one of the state prosecutors, 'investigation indicates that this was a professionally set up criminal campaign, which pointedly exploited the high pressure of companies and the government alike to cope with the corona crisis'.[110] Investigations into over 104 sites, with links to servers in Slovakia and the US, are ongoing.[111] The scale and speed with which these fraudulent websites were set up provides an indication of how OCGs can leverage their global networks and access to specialised expertise to acquire and process thousands of datasets for fraudulent purposes.

These cases highlight not only the agility of OCGs to exploit new and emerging vulnerabilities but also the transnational nature of organised fraud and the ability of OCGs to commit fraud on a massive scale using global networks. This often automatically places the investigation beyond the capacity of local police forces operating in isolation.

Professionally Enabled Fraud

In contrast to the professionally organised frauds described above, some require a higher degree of sophistication to facilitate fraud that is committed under the guise of legitimate business practices. The very nature of these frauds dictates OCG involvement, due to the need for the involvement of specialist professional enablers working in concert with lead perpetrators.

There are several ways in which OCGs can come to possess this level of sophistication. For example, criminals have been known to organise annual conferences with other established and would-be fraudsters where scam typologies, data lists, and the latest law enforcement tactics are discussed and sold onto fellow criminals.[112] Furthermore, fraudsters deliberately seek to employ or corrupt professionals in the fields of finance, accounting and law to provide

108. See NAO, 'Investigation into the Bounce Back Loan Scheme', 7 October 2020, <https://www.nao.org.uk/report/bounce-back-loan-scheme/>, accessed 7 October 2020.
109. Karin Matussek, 'Germany's Corona Aid Was Fast – But So Were the Fraudsters', *Bloomberg*, 15 April 2020.
110. *Ibid.*
111. Guy Chazan, 'Germany Cracks Down on Coronavirus Aid Fraud', *Financial Times*, 19 April 2020.
112. Author interview with law enforcement agency, August 2020.

the expert knowledge and veneer of respectability required to perpetrate the crime.[113] These professional enablers are key in making OCG activities 'more difficult to detect and uproot'.[114]

Case Study: Pension Liberation Frauds

Pension liberation frauds involve misleading an individual to access their pension funds, without informing them of the potential tax liabilities, in order to induce them to invest the monies in supposedly high-return schemes.[115] Recent research conducted by the Police Foundation found 13 pension companies reported a total of 938 customers with aggregate savings amounting to £54 million who were targeted by scammers in 2019 alone. Sixty-two percent of these customers had insisted on the transfer regardless of the risk, with £31 million potentially lost.[116]

Just as with the coronavirus crisis, here criminal groups have demonstrated their ability to respond decisively to changes in the public policy environment following reforms to UK pension law in 2015. These allowed individuals to access their pension pot from age 55 without investment in an annuity or drawdown pension.[117] Although designed to offer individuals greater control over their retirement planning, interviews suggest that OCGs were quick to adapt to the changes in order to target this new flexibility. The full scale of OCG involvement is yet to be fully understood. However, interviewees for this research noted that 'investment frauds, particularly those which target pension liberation schemes introduced in 2016, are a high-harm fraud type, and a priority for us. It is an area where organised crime is strongly present'.[118]

What is known is that criminals use sophisticated mass marketing and social engineering techniques to approach individuals directly with offers of free pension reviews and promises of abnormally high returns on an investment.[119] However, in order to understand how OCGs exploit these situations, it is necessary to recognise the network of enablers that provide the legitimisation needed to make the frauds successful. In research by the Police Foundation, one of the case studies detailed 'a loose cartel of enablers and businesses across the UK with an organised crime group at its centre, with links to other crimes such as serious violence and money laundering as well as numerous fraudulent pension companies'.[120]

113. See, for example, Action Fraud, '"Fraudster Families" Running Multimillion Pound Pension Scams', 12 February 2019, <https://www.actionfraud.police.uk/news/fraudster-families-running-multimillion-pound-pension-scams>, accessed 7 October 2020.
114. International Public Sector Fraud Forum, 'Guide to Understanding the Total Impact of Fraud', p. 5.
115. Michael Skidmore, 'Protecting People's Pensions: Understanding and Preventing Scams', The Police Foundation, September 2020, p. 2.
116. *Ibid.*, p. 3.
117. See HM Revenue and Customs, 'Pension Changes 2015', <https://www.gov.uk/government/news/pension-changes-2015>, accessed 7 October 2020.
118. Author interview with senior law enforcement professional, June 2020.
119. Citizens Advice, 'Too Good to be True? Understanding Consumer Experience of Pension Scams a Year on from Pension Freedoms', 2016.
120. Skidmore, 'Protecting People's Pensions', p. 19.

Several layers of deception are needed to make the schemes sufficiently convincing to other pension companies and industry regulators as well as potential victims. This includes duplicating business strategies and product marketing tactics seen in the legitimate sector, acquiring some form of authorised status from regulators, and onboarding legitimate professionals into their illicit activities.[121]

The nature of this fraud has led it to be described as a 'ticking time bomb';[122] the true scale of the damage will not be revealed to the victim for several years when, upon planning to retire, they find that their investments are worthless. This means the current reactive/victim-led model for fraud investigation is an inadequate response to this type of fraud. The sophistication of the crime requires a much more intelligence-led, proactive response centred around the OCG, rather than the reporting victim.

Project Bloom, a cross-agency taskforce headed by the Pensions Regulator, has been set up to tackle the issue of pension liberation fraud.[123] Early results from this approach are positive,[124] but greater access to the specialist assets available in SOC policing would be valuable to this effort.

The impact of allowing this organised fraud type to fester is clear – it leaves victims either unable to retire or reliant on the state for support in their old age, thus placing an increased burden on public finance.

Attacking Fraud Through the Organised Crime Response

Exploring what is known – and what is unknown – about 'fraud as an organised crime' points to a need for major reforms to both the standing of fraud within the SOC intelligence and policing response and the way that fraud investigations are used to target 'the soft underbelly of organised crime'.[125]

Interviews for this paper repeatedly reaffirmed that it is difficult for fraud investigators to access the specialist skills, covert tactics and bandwidth of the broader intelligence architecture that are commonly used in the response to other SOC threats, such as drug and people trafficking.[126] A starting point for addressing this is the removal of operational and informational silos between

121. *Ibid.*, p. 16.
122. Author interview with counter-fraud professional, September 2020.
123. See Department for Work and Pensions et al., 'Government Warning: Arm Yourself with the Facts, Don't Lose Your Pension to Scammers', 27 July 2015, <https://www.gov.uk/government/news/government-warning-arm-yourself-with-the-facts-dont-lose-your-pension-to-scammers>, accessed 7 October 2020.
124. Maria Espadinha, 'Warning of Fraudster Families Running Pension Scams', *FT Adviser*, 12 February 2019.
125. Author interview with law enforcement professional, August 2020.
126. Author telephone and video interviews with serving and former law enforcement professionals, June–September 2020.

the fraud and SOC policing worlds. Only then can the system start to move from its current 3% investigation rate towards the higher rates needed to rebalance the risk–reward equation in the minds of offenders.

Breaking Down Operational Silos

Interviews suggest that some of the necessary changes in prioritisation of fraud within the SOC response can in part be achieved by impactful yet simple changes within law enforcement.[127] For example, there is currently an operational silo between the organised crime and fraud responses within the National Police Chiefs' Council,[128] the body responsible for coordinating the work of UK police forces. Although fraud requires its own specific focus within this structure, more could be done to integrate the two disciplines. However, a police force lead model is unlikely to achieve the step-change required, whereas placing the authority at the NCA level with a national responsibility could. Furthermore, despite being named as a facet of SOC in the UK government's Serious and Organised Crime Strategy 2018[129] and referenced in the Strategic Policing Requirement,[130] which guides priority areas for the police, fraud continues to be under-represented in the SOC policing response.[131] One way to remedy this would be to place a more specific responsibility on forces to prioritise organised fraud within their SOC response.

Recommendation 7: The Strategic Policing Requirement should be amended to emphasise fraud as a SOC priority, led by the NCA, to ensure specialist resources are available for the investigation of serious and organised fraud.

Breaking Down Informational Silos

The fragmented intelligence picture surrounding 'fraud as an organised crime' is the result of not only a lack of operational prioritisation, but also continuing informational silos between various tranches of the public, private and third sectors. Although interviews noted the good progress in data-matching efforts between public and private fraud-specific data,[132] more could be done to build informational pathways between fraud and organised crime datasets as a route to better understanding the specific scale and nature of the organised fraud threat.

Public–private information-sharing models in other areas, such as the Joint Money Laundering Intelligence Taskforce (JMLIT),[133] which provide clear gateways between the public and private

127. Author video interview with senior law enforcement professional, August 2020.
128. HM Government, *Serious and Organised Crime Strategy*.
129. *Ibid.*
130. Home Office, 'The Strategic Policing Requirement', March 2015.
131. Author interview with senior law enforcement professional, June 2020.
132. Author video interviews with counter-fraud professionals, June–August 2020.
133. See NCA, 'National Economic Crime Centre', <https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed 7 October 2020.

sectors,[134] could provide a useful template and a starting point for better coordination. The recent establishment by the NECC of a 'Public–Private Operational Board', which aims to bring better coherence to public–private information sharing on fraud, money laundering and cyber threats, shows a move towards greater cross-disciplinary data-matching.[135] Breaking down the informational silos between fraud and SOC should be a key goal of the new board.

Recommendation 8: A key goal of the NECC's Public–Private Operational Board should be greater cross-dataset exploitation between fraud and SOC as a means of better understanding the threat from organised fraud.

134. Section 7 of the Crime and Courts Act 2013 provides broad powers of information sharing between the private sector and the NCA, and provides the legal information-sharing gateway for the JMLIT.
135. The NECC houses the UK's independent Financial Intelligence Unit with its database of suspicious activity reporting and sits within the NCA, which has access to a broad range of data relating to serious and organised crime. Research and interviews with senior NECC officials in October 2020 highlighted the establishment of the Public–Private Operational Board. No publicly available information about its future role and remit are available.

III. Fraud and Terrorist Financing

ALONGSIDE SOC, TERRORISM is a clear UK national security threat and the focus of major government spending.[136] Typically, however, when terrorist financing is considered by policymakers and the private sector, it has been linked to the methods used by Al-Qa'ida at the time of 9/11 (donors, charities and the formal banking sector); the business ventures of Lebanese Hizbullah; the charcoal export of Al-Shabaab in Somalia; the oil exploitation of the Islamic State; or even the cattle rustling of Boko Haram.[137] This is not surprising as these groups have loomed large in the global security dialogue and either finance themselves from the territory and populations they control or run sophisticated organised crime operations.[138] On this basis, these groups have little reason to resort to fraud as a key source of funding.

However, as the form of terrorism has evolved from group-based, centrally funded missions – such as those of Al-Qa'ida at the time of 9/11 – to attacks conducted by lone actors or small cells,[139] be they Islamist, right-wing or single-issue-based (such as animal rights), some are suggesting that 'fraud has now become the crime of choice for terrorists who have acquired funding via benefit and credit card fraud, identity theft and the sale of counterfeit goods'.[140] Indeed, as illustrated below, some literature from those promoting terrorism advocates the use of fraud as a fundraising tool, providing relevant examples of the widely considered crime–terror nexus.[141]

In the case of the jihadi terrorist, taking the wealth of what they would label as 'disbelievers' is central to the raising of finance and thus fraud is considered an accepted fundraising tool. For example, in the Winter 1431/2010 edition of Al-Qa'ida in the Arabian Peninsula's (AQAP)

136. HM Treasury, *Budget 2020* (London: The Stationery Office, 2020), para. 1.37.
137. Financial Action Task Force (FATF), Inter-Governmental Action Group Against Money Laundering in West Africa and Task Force on Money Laundering in Central Africa, 'Terrorist Financing in West and Central Africa', October 2016, p. 12.
138. For an extensive review of terrorist financing typologies, see Tom Keatinge and Florence Keen, 'A Sharper Image: Advancing a Risk-Based Response to Terrorist Financing', *RUSI Occasional Papers* (March 2020).
139. Tom Keatinge and Florence Keen, 'Lone-Actor and Small Cell Terrorist Attacks: A New Front in Counter-Terrorist Finance?', *RUSI Occasional Papers* (January 2017).
140. Francesca Cassidy, 'How Fraud is Funding Terrorism', *Raconteur*, 7 September 2018, <https://www.raconteur.net/risk-management/fraud-funding-terrorism>, accessed 30 October 2020.
141. See, for example, Tamara Makarenko, 'Crime–Terror Continuum: Tracing the Interplay Between Transnational Organised Crime and Terrorism', *Global Crime* (Vol. 6, No. 1, February 2004), pp. 129–45; Global Counterterrorism Forum, 'The Hague Good Practices on the Nexus Between Transnational Organized Crime and Terrorism', <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2018/GCTF-Good-Practices-on-the-Nexus_ENG.pdf?ver=2018-09-21-122246-363>, accessed 19 December 2020; UN Security Council Resolution 2482.

English-language magazine *Inspire*, then AQAP leader Anwar Al-Awlaki wrote a six-page justification entitled 'The Ruling on Dispossessing the Disbelievers [sic] Wealth in Dar Al-Harb'.[142] Beyond this foundation, the importance of fraud as a tool for terrorist financing is clearly illustrated in a 2015 guide purportedly produced by a supporter of the Islamic State who had 'been studying the global Jihad for 10+ years'.[143] This guide covers many of the different forms of fraud that this chapter will explore. In a section entitled 'Earning Money',[144] the author provides advice on a range of fraud-based methods for earning 'easy money'. This includes encouraging credit card fraud, PayPal/eBay scams, phishing and hacking, as well as claiming 'extra benefits from a government' and avoiding paying taxes. The author also reports – without evidence – that 'a Muslim Accountant "took" $50 million dollars [sic] from his boss and fled to the Islamic State';[145] and that '[a]nother Muslim hacked some Israeli credit cards and used the money to go [to] the Islamic State'.[146] Although this document is, perhaps, fanciful, it certainly provides an insight into the role fraud can play in terrorist financing, as evidenced by the real-life cases explored in the rest of this chapter.

To draw attention to the contemporary use of fraud as a terrorist financing tool is not to suggest that fraud is a new means by which terrorist actors fund themselves,[147] nor is it to suggest that it is only lone actors and small cells that resort to this form of funding. For example, in the 1980s, terrorists on both sides of the conflict in Northern Ireland reportedly coerced construction subcontractors to commit tax fraud for fundraising purposes, with a judge noting at the time that both Protestant and Catholic terrorists were being financed with 'untold millions of pounds … in British taxpayers' money'.[148]

With this framing in mind, and to understand the full picture of how fraud impacts UK national security, this chapter will demonstrate, through the use of case studies, the past and emerging centrality of fraud to terrorist financing as both a fundraising tool and a tool in the counterterrorism armoury.

Before progressing, it is important to consider what is meant by 'terrorist financing' in this chapter. As noted above, it is typically considered to cover the raising of significant funds to support the operations of terrorist groups – for example, in the case of Al-Qa'ida, this includes training camps, recruitment and propaganda activity, as well as attacks themselves.

142. Anwar Al-Awlaki, 'The Ruling on Dispossessing the Disbelievers Wealth in Dar Al-Harb', *Inspire* (No. 1431, Winter 2010).
143. 'How to Survive in the West: A Mujahid Guide', 2015, p. 6.
144. *Ibid.*, pp. 13–15.
145. *Ibid.*, p. 14.
146. *Ibid.*
147. The FATF's 2008 study on terrorist financing reveals a range of ways in which fraud has been used to finance terrorism, including cheque and credit card fraud and defrauding donors to charities. See FATF, 'Terrorist Financing', 29 February 2008.
148. *Associated Press*, 'Judge Says Tax Fraud Finances Terrorism', 12 February 1987.

As will be clear from the cases illustrated below, however, fraud is typically (although not exclusively) a tool used by what have become known as 'lone actors and small cells'.[149] This category of terrorist actor spends little on their attacks, relying on low-cost methods such as knives or vehicle-based attacks. For them, fraud represents a means of subsistence, to 'fund the terrorist, not fund the attack'.[150] Furthermore, although not covered elsewhere in this paper given the restricted focus on fraud for financial gain, it is important to note the role that identity fraud can play in facilitating terrorist financing[151] by providing the documentation needed to secure benefits and access to other forms of financing.

During the process of gathering case studies in support of this research, it became evident that the links between terrorist financing and fraud are broad and diffuse in nature, with case studies revealing a wide sweep of targets and methodologies of fraud perpetrated against individuals, the state and the private sector. In short, no potential source has been left unexploited. The following case studies – grouped by victim sector – serve to highlight the breadth and variety of fraud as a terrorist financing tool.

Fraud Against Individuals

As the case studies below demonstrate, individual citizens of the UK have repeatedly been targets for fraud as a means of funding terrorism. The methods are diverse, however the common theme which emerges is that these particular fraud typologies are not unique to terrorists, but echo established fraud schemes in the SOC sphere. In this way, as reviewed later in this chapter, fraud-based law enforcement responses to terrorist financing may be able to take learnings from the approaches taken to tackling fraud beyond the counterterrorism sphere.

Case Study: Courier Fraud

Perhaps one of the most notable terrorist financing frauds, perpetrated by supporters of the Islamic State against individuals, came to be known as the 'Bank of Terror' fraud.[152] In this case, eight men were convicted of defrauding UK pensioners out of more than £1 million that was alleged by police to be used in part to fund travel from the UK to Syria to join the Islamic State. The fraud, often referred to as 'courier fraud', involved calls placed to the victims by individuals posing as police officers. During the call, the fraudsters would persuade the victim that their existing bank account was compromised and that their bank balance should be transferred to another account (controlled by the fraudsters) or withdrawn and handed to a member of the gang masquerading as a police officer for safekeeping. During the trial, it was revealed that

149. Keatinge and Keen, 'Lone-Actor and Small Cell Terrorist Attacks'.
150. Author video interview with former UK law enforcement officer, 1 July 2020.
151. FATF, 'Financing of Recruitment for Terrorist Purposes', January 2018, p. 18; Public–Private Analytical Exchange Program, 'Counterterrorism Futures: A Whole-of-Society Approach', 17 October 2019, <https://www.dhs.gov/sites/default/files/publications/ia/ia_counterterrorism-futures.pdf>, accessed 9 October 2020; author video interview with former UK law enforcement officer, 1 July 2020.
152. *The Guardian*, '"Bank of Terror" Conmen had Catastrophic Impact on Victims, Court Told', 29 April 2016.

5,695 calls had been made to 3,774 different numbers leading to approximately 140 frauds or attempted frauds.[153]

Case Study: Online Sales-Based Fraud

A further high-profile means by which terrorists and their supporters have raised funds is through online sales-based fraud, notably scams perpetrated via the online auction site eBay. One case in particular illustrates the effectiveness of this type of fraud for fundraising.

In October 2018, Hassan Butt – who claimed to have recruited over 200 jihadists to attend terror training camps[154] – was convicted in the UK of fraudulent trading involving a scam in which he used eBay to advertise the sale of electronic goods by his company MI Genie. At trial, the court heard that, '[i]n a 10-day period in December 2014 the company took £1.1m of orders but no items were delivered and the money disappeared',[155] with approximately 3,000 members of the public falling victim to the fraud. He committed further online sales-based fraud by ordering £6,000 worth of high-value goods (including iPads and gold bars) for himself and then falsely obtaining refunds by claiming that the goods never arrived.[156]

In addition to providing fraudulent fundraising opportunities, online sales websites can also be used to camouflage money transfers between connected parties, as in the case of Mohamed Elshinawy who received funds from overseas co-conspirators 'to be used to conduct a terrorist attack in the United States'.[157] In this case, one way in which Elshinawy hid the receipt of funds was to falsely disguise them as a payment from a UK Company (iBacs Ltd) with which he was connected, for the purchase of two printers.

From these two cases, the vulnerability of online sales platforms to fraud and abuse in support of terrorist financing is clear, which highlights the extent to which terrorist financing activity spreads far beyond the traditional tools – predicated on those favoured by Al-Qa'ida – that are most often the focus of the counter-terrorist financing responses of national governments.

Identity Theft

Although this paper is primarily focused on fraud for financial gain, it is important to recognise that a key element of many of the cases of fraud reviewed for this chapter is identity theft. In modern economies, proof of identity unlocks access to a range of financial benefits including social security payments, opening of bank accounts, and access to credit cards and other

153. *BBC News*, 'Gang Jailed Over Pensioner Phone Scam', 4 May 2016.
154. *BBC News*, 'Hassan Butt: Conman Who Claimed to Have Recruited Jihadists Jailed', 5 October 2018.
155. Chris Dawson, 'eBay Fraudster Jailed for 13 Years for £1.1m Scam', *Tamebay*, 5 October 2018.
156. Sophie Halle-Richards, 'The Bury-Based eBay Fraud That's Left PayPal £1m Out of Pocket', *Manchester Evening News*, 5 October 2018.
157. US vs. Mohamed Elshinawy, 'Memorandum Opinion', US District Court for the District of Maryland, 28 March 2018, p. 17.

financial services. While this form of fraud has been used for financial gain for many years, as the Islamic State guidance noted earlier illustrates, fraud has become a key method by which lone actors and small cells raise funding. It thus follows that identity theft to commit fraud has become increasingly prevalent among those with terrorist intent, including for the purchase of fraudulent identification documents such as driving licences and passports. As noted in a testimony by the FBI to the US Congress, identity theft 'can be utilized by terrorists to obtain Driver's Licenses, and bank and credit card accounts through which terrorism financing is facilitated', underlining that '[i]dentity theft is a key catalyst fuelling many of these [funding] methods'.[158] Fraudulent documents, or 'fraudulently obtained genuines', also provide terrorists with access to secure areas, be that entry into a target country or access to restricted areas such as the air-side zones within airports.[159] As one terrorism investigator has observed, '[f]or these [terrorist] groups, passports are as important as weapons'.[160]

Recommendation 9: The government should actively revisit the role that effective digital ID schemes can play in protecting against all forms of fraud, including as a tool for countering fraud for terrorist financing purposes, as part of its National Data Strategy.[161]

Fraud Against the State

The extent to which fraud presents a risk to public finances and the UK's national prosperity has been set out earlier in this paper. However, fraud against public finances also presents a real and present risk in terms of terrorist financing. Broadly speaking, this threat can be divided into two sub-groups, namely, fraudulent claims for social security support and tax and excise frauds. Furthermore, in contrast to criminal fraud against the state conducted for profit, in terrorist cases it most often funds living expenses.

Fraudulent Claims for Social Security Support

In an era of small cell and lone actor fraud, as noted above, there is a need to 'fund the terrorist, not the act'. As a result, benefit and student loan frauds have emerged as a key risk.

158. FBI, 'Testimony: John S Pistole, Assistant Director, Counterterrorism Division, FBI, Federal Bureau of Investigation Before the House Select Committee On Homeland Security, Washington DC, October 2003', <https://archives.fbi.gov/archives/news/testimony/fraudulent-identification-documents-and-the-implications-for-homeland-security>, accessed 31 August 2020.
159. *Ibid.*
160. Oriana Zill, 'Crossing Borders: How Terrorists Use Fake Passports, Visas, and Other Identity Documents', PBS Frontline, <https://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html>, accessed 31 August 2020.
161. Department for Digital, Culture, Media and Sport, 'Guidance: National Data Strategy', 8 July 2019, <https://www.gov.uk/guidance/national-data-strategy>, accessed 31 October 2020.

Case Study: Benefit Fraud

Benefit (and related) fraud has provided valuable funding to terrorist actors, allowing them to conduct attacks but also, importantly, to live without working or engaging with wider society. Not all benefit-related terrorist financing is necessarily linked to fraud – in some cases payments are a function of system failures.[162] For example, the £3,000 of UK housing benefit handed to Mohamed Abrini – who is alleged to have been involved in both the 2015 Paris and 2016 Brussels terrorist attacks – was reportedly the result of an erroneous overpayment that was withdrawn via fraudulent means from the account of a foreign terrorist fighter who had travelled to Syria and was then passed to Abrini.[163] But defrauding the benefits system in societies that provide generous financial support to those that can prove legitimate need (albeit through fraudulent evidence) has become a popular means by which those with terrorist intent can finance their lives as they prepare their attacks. This poses challenges to societies for which the provision of welfare to their citizens is a priority, one they may be loath to securitise.

Case Study: Student Loan Fraud

As the era of jihadi foreign terrorist fighters dawned, given the profile of many of the travellers, one form of fraud against the state in the UK was going to prove particularly supportive, namely the provision of student loans. While some form of student support is paid directly to the educational institution, others (primarily maintenance loans) are paid to the student. As an interviewee noted in 2015, 'we do not monitor what students do with the funds we provide to them under the student loan scheme; they can drink it all in the bar on the first night of term. We do however seek to ensure that the loan application is legitimate'.[164] This vulnerability in the system meant that if applicants could successfully prove the legitimacy of their application, the UK government would provide funds which were used to pay for their travel to Syria and Iraq.

This form of fraud-based terrorist financing is illustrated by the case of Yahya Rashid, who was charged with having fraudulently gained a place at Middlesex University using a forged BTEC certificate, secured a £6,000 student loan as a result and then purchased airline tickets to Morocco for himself and four others as part of their circuitous travel route to Syria.[165]

The case of Salman Abedi, the 2017 Manchester Arena bomber, provides a further example of the abuse of the student loan system. He received several tranches of funding, including at least one despite having dropped out of his course.[166] This case shines a light on an inherent

162. Mark Maremont and Valentina Pop, 'Terrorist Suspects in Europe Got Welfare Benefits While Plotting Attacks', *Wall Street Journal*, 4 August 2016.
163. Duncan Gardham, '£5,000 in Mispaid Housing Benefit "Used to Fund Isis Terror Cell"', *The Guardian*, 25 November 2016.
164. Author interview with London-based civil servant, July 2015.
165. In the Court of Appeal (Criminal Division) on appeal from the Crown Court and Central Criminal Court, R v Yahya Rashid and others, EWCA Crim 568, May 2016, pp. 24–25.
166. *BBC News*, 'Manchester Arena Bomb Parts "Bought by Brothers Using Mum's Card"', 10 February 2020.

vulnerability in the student loan monitoring system because, as the Student Loans Company noted to *The Daily Telegraph* in the aftermath of the bombing, 'it is for universities to inform the Student Loans Company when students withdraw or suspend their studies, at which point funding stops'.[167]

Recommendation 10: Agencies charged with distributing benefits and government support should receive basic training on how to identify terrorist financing vulnerabilities and should make greater use of tech-based tools, such as IP address monitoring and geo-location tools, to ensure service users' locations are consistent with their supposed status.

Furthermore, lessons from the abuse of student loan funds should be considered to develop measures for ensuring the integrity of their use.

Tax and Revenue Fraud

A further example of government agencies that are at risk of inadvertently financing terrorism are tax and revenue agencies. Although these bodies are well attuned to fraud risks, greater understanding of the specific typologies associated with terrorist financing-related fraud may help to minimise this risk.

Case Study: Tax Credits and Rebates

The case of Jonathan Paul Jimenez in the US in 2013 highlights this vulnerability. Jimenez was sentenced to 10 years in prison in connection with international terrorism and conspiring to defraud the US tax authority, the Internal Revenue Service (IRS), by submitting a false tax return claiming three children as his dependents and thus receiving an associated $5,587 refund from the IRS.[168]

An additional, eye-catching case of terrorist financing-related tax fraud, reported by the press in 2019, concerns Missing Trader Intra Community Fraud (MTIC), informally referred to as 'carousel fraud'. These frauds allow perpetrators to claim VAT rebates and are estimated to cost the EU at least €60 billion per year in lost tax revenue.[169] In this case, according to reporting by

167. Robert Mendick, Martin Evans and Victoria Ward, 'Manchester Suicide Bomber Used Student Loan and Benefits to Fund Terror Plot', *Daily Telegraph*, 27 May 2017.
168. FBI, 'Man Sentenced to 10 Years in Federal Prison for Lying in Terrorism Investigation and False Claim Conspiracy', press release, 19 April 2013, <https://archives.fbi.gov/archives/tampa/press-releases/2013/man-sentenced-to-10-years-in-federal-prison-for-lying-in-terrorism-investigation-and-false-claim-conspiracy>, accessed 18 December 2020.
169. For an explanation of the workings of MTIC fraud, see Europol, 'MTIC (Missing Trader Intra Community) Fraud', <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud>, accessed 5 October 2020.

The Sunday Times, a multi-billion-pound MTIC scheme was used to defraud the UK government, and a portion of these proceeds was alleged to be used to finance terrorism.[170]

Case Study: Gift Aid

Another form of tax fraud involves the abuse of charitable organisations. The role of charitable bodies as a vehicle for terrorist financing has been extensively covered elsewhere,[171] so for the purposes of this paper, the association of charities with terrorist financing will be limited to their role in committing fraud against a state.

In the UK, charities benefit from a number of tax benefits, including the 'gift aid' scheme[172] under which they can reclaim the income tax paid on donations they receive from the general public. Inevitably, consistent with the advantage terrorists have taken of other forms of government rebate, gift aid presents an attractive opportunity for those using charities to support terrorism-related fundraising. Although cases are rare, the risk is not imagined as those charities that have been found to be abused for terrorist financing purposes are likely to have benefited from the government's gift aid scheme,[173] and the cases of gift aid fraud that have been prosecuted indicate the extent to which large sums can be raised via this method.[174]

Case Study: Excise Fraud

A final tax-based fraud popular with terrorist groups – particularly those operating organised crime-type operations[175] such as Hizbullah[176] and Dissident Republicans in Northern Ireland[177] – is excise fraud, in particular taking advantage of tax differentials on high-duty items such as cigarettes and fuel between countries or states.

170. Tom Harper, Madlen Davies and Ben Stockton, 'Named: British Men "Linked to Spies, Terrorists, Sheikhs and £8bn Fraud"', *Sunday Times*, 9 June 2019.
171. FATF, 'Risk of Terrorist Abuse in Non-Profit Organisations', June 2014.
172. See HM Government, 'Claim Gift Aid Online', <https://www.gov.uk/claim-gift-aid-online>, accessed 8 October 2020.
173. Andrew Gilligan, '"Terror Link" Charities Get British Millions in Gift Aid', *Daily Telegraph*, 29 November 2014.
174. See, for example, David Ainsworth, 'Twins Jailed for £450,000 Gift Aid Fraud', *Civil Society News*, 27 March 2018.
175. For a discussion of the terrorist financing methods adopted by different forms of terrorist groups, see Keatinge and Keen, 'A Sharper Image'.
176. *BBC News*, 'Two Guilty of Smuggling for Hezbollah', 22 June 2002.
177. FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom – Mutual Evaluation Report', December 2018, p. 19.

For example, in 2002, two brothers were convicted of financing Hizbullah by smuggling cigarettes from the low-tax US state of North Carolina for resale in higher-tax states such as Michigan, with the net profit smuggled to support Hizbullah.[178]

More recently, in Northern Ireland, the Police Service of Northern Ireland and HMRC collaborated to target the sale of illicit tobacco products in support of the paramilitary group the Irish National Liberation Army (INLA), noting that customers that purchase illicit cigarettes 'should be aware that they may be indirectly funding INLA terrorism and criminality which brings harm to local communities, for their own selfish gains'.[179]

Case Study: Coronavirus-Related Fraud

While it is perhaps too early to identify any particular coronavirus-related fraud trends with links to terrorism, there is no doubt that considerable opportunity for such fraud exists as governments seek to deliver financial aid to individuals and companies as rapidly as possible. For example, German law enforcement is reportedly investigating an individual in Berlin, with links to a militant Islamist movement, for 'exploiting the corona crisis' and defrauding the support scheme of €18,000.[180]

As can be seen from this collection of case studies, terrorist financing-related fraud against the state falls into two main categories: the fraudulent securing of benefits, often through the use of fraudulent documentation to justify fraudsters' entitlement to the benefit; or securing tax payments due to the government for the terrorists' own benefit. Given this profile, the UK's National Terrorist Financial Investigation Unit (NTFIU) has always benefited from the intelligence dividend and focus provided by embedded staff from HMRC and the Department for Work and Pensions. Currently, however, the sustainability and lasting nature of these links appears open to question.

Recommendation 11: Embedded positions for HMRC and Department of Work and Pensions staff in the NTFIU should be maintained to help spot fraud disruption opportunities.

178. *BBC News*, 'Two Guilty of Smuggling for Hezbollah'.
179. *BBC News*, 'Police Seize 30,000 Illegal Cigarettes in Anti-INLA Raids', 25 February 2019.
180. Chazan, 'Germany Cracks Down on Coronavirus Aid Fraud'.

Fraud Against the Private Sector

The private sector is not immune to abuse of fraud as a terrorist financing tool. Indeed, as is the case with fraud against individuals or the state, this paper notes that terrorists have not sought to reinvent the wheel in their approach to fraud against business as a terrorist financing tool; terrorists have by and large adopted typologies and schemes that have been put to use by OCGs and repurposed them as tools to support their own activities. Many of the schemes themselves are indistinguishable on paper from those perpetrated by OCGs, despite the ultimate driver for fundraising being different. In this way, closer cooperation and intelligence sharing between fraud, organised crime and counterterrorism policing may be desirable.

Case Study: Credit Card Fraud

Credit card fraud appears repeatedly as a form of terrorist financing, particularly for the funding of large cost items, such as airline tickets. The nature of credit cards means that fraudulent purchases made with stolen card details, or purchases made with fraudulently acquired cards, are often not identified until the fraudster has had the opportunity to make use of their purchase. For example, in 2016, Ghulam Hussain was arrested under the UK Terrorism Act 2006 for the preparation of terrorism acts, having confessed to an undercover officer that he intended to travel to join the Islamic State, funding his travel and other activity through fraudulently obtained credit cards,[181] which he secured by inflating his income.[182]

Another example of terrorism-related credit card fraud is provided by a 2007 case where UK-based supporters of the Tamil Tigers operating up to 200 independently owned petrol stations were alleged to be skimming data from drivers' credit cards during payment, before cloning the cards and using them to withdraw funds from ATMs around the world.[183]

Case Study: Fraudulently Obtained Banking Loans

A common theme in fraud against the private sector is the fraudulent application for and receipt of credit via loans (often against the inflated value of property or income), after which the applicant defaults on the loan, having transferred the excess funds to a terrorist organisation. One such example is provided in the US by the prosecution of Khalid Ouazzani, who pleaded

181. *Yorkshire Live*, 'Man Who Told Undercover Officers He Was Planning to Join ISIS in Syria is Jailed', 4 August 2017.
182. Crown Prosecution Service, 'The Counter-Terrorism Division of the Crown Prosecution Service (CPS) – Successful Prosecutions Since 2016', <https://www.cps.gov.uk/crime-info/terrorism/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-2016>, accessed 26 August 2020.
183. Sean O'Neill, 'Petrol Station Scam "Was Masterminded by the Tamil Tigers"', *The Times*, 23 April 2007.

guilty to submitting false financial information to obtain a business loan from a number of US-based banks,[184] and then at a later date provided $23,000 for the use and benefit of Al-Qa'ida.[185]

Although fraud has not received the headlines that other forms of terrorist financing have secured in recent years, studies of terrorist financing by national governments and international organisations have not overlooked this threat, even if responses have prioritised other forms of terrorist financing.[186]

For example, a 2008 terrorist financing report from the Financial Action Task Force (FATF) – the global anti-money laundering and counterterrorist financing standard-setter – emphasised the role of fraud in terrorist financing by providing a number of fraud-based examples, including: the role of online financial fraud via hacking credit cards;[187] the fraudulent abuse of charitable donations, including fraudulently obtaining grants from a government agency;[188] and low-level crime via credit card and cheque fraud.[189]

While these forms of fundraising may individually not match the commercial fundraising activity of groups such as Al-Shabaab or the Islamic State, over time they can be highly effective and provide funds necessary for terrorists to operate. These issues should be considered when implementing counter-fraud systems and controls and, as discussed below, when designing the counterterrorism response.

Fraud as a Counterterrorism Response

Thus far in this chapter, fraud has been considered as a funding tool for terrorist actors. However, by the same token, fraud could be considered as a vulnerability for terrorists and a means of disrupting their activity.

184. US v. Khaled Ouazzani, Case No. 10-00025-01-CR-W-HFS (Indictment) (W.D. Mo. February 2010).
185. FBI, 'Al Qaeda Supporter Pleads Guilty to Supporting Terrorist Organization', press release, 19 May 2010, <https://archives.fbi.gov/archives/kansascity/press-releases/2010/kc051910.htm>, accessed 18 December 2020.
186. The UK's 2017 'National Risk Assessment of Money Laundering and Terrorist Financing' treats the issue in passing with a footnote. See HM Treasury and Home Office, 'National Risk Assessment of Money Laundering and Terrorist Financing', October 2017, p. 27. The latest UK National Risk Assessment describes fraud as a 'far less prevalent method'. See HM Treasury and Home Office, 'National Risk Assessment of Money Laundering and Terrorist Financing', December 2020, p. 44. Other governments that consider fraud as a tool of terrorist financing include: US Department of the Treasury, 'National Terrorist Financing Risk Assessment: 2015'; Australian Transaction Reports and Analysis Centre, 'Terrorism Financing in Australia 2014'; Government of Israel, 'National Risk Assessment on Terror Financing', 2017; Dutch Ministry of Justice and Security, 'National Risk Assessment of Money Laundering and Terrorist Financing 2017'.
187. Financial Action Task Force, 'Terrorist Financing', p. 9.
188. *Ibid.*, p. 12.
189. *Ibid.*, p. 15.

Due to the complexities of meeting evidential thresholds for terrorism charges, in many of the cases cited above, the ultimate criminal justice response by the authorities to a terrorism case was a fraud charge. A good example of the considerations applied to these cases is a 2009 case involving the mobile phone filming of potential terrorist attack targets by an Algerian man posing as a tourist in London. Investigations revealed that he and his brother purchased £5,000 worth of mobile phones using a fraudulent credit card. Although the brothers were arrested and held under the Terrorism Act, they were ultimately charged with fraud offences as, according to press reports, 'aspects of the [terrorism] law were being challenged in the House of Lords at the time and the fraud offences carried roughly the same penalties'.[190] A further, ongoing case in Northern Ireland likewise shows how fraud-based action can be used for disruption purposes; Operation *Attina* includes the freezing of a property associated with the alleged head of a Republican paramilitary group.[191]

These cases highlight the role that fraud detection and prosecution can play in counterterrorism, a response amply illustrated by data (see Table 2) provided by the UK to the FATF for its Mutual Evaluation Report (MER).[192]

190. Sean O'Neill, 'Beat Officers "Prevented Terror Attack by Stopping Suspicious Tourist"', *The Times*, December 2009.
191. NCA, 'NCA Northern Ireland Performance: Q1 2018/19 (April – June 2018)', 22 August 2018, p. 6.
192. Approximately every 10 years, the FATF conducts a review of the extent to which a country is complying with, and effectively implementing, globally agreed anti-financial crime standards. The UK's most recent review was published by the FATF in December 2018. See FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom – Mutual Evaluation Report'.

Table 2: Common Criminal Alternatives to a Terrorist Financing Prosecution

	2013/14	2014/15	2015/16
Prosecutions			
Common Law Fraud Offences	0	3	0
Criminal Law Act 1977 Fraud Offences	0	2	16
Fraud Act 2006	6	13	22
Proceeds of Crime Act 2002	10	6	17
Total Alternative Prosecutions	*16*	*24*	*55*
Total Terrorist Financing Prosecutions (England, Scotland and Wales)	*N/A*	*47*	*89*
Convictions			
Common Law Fraud Offences	2	1	0
Criminal Law Act 1977 Fraud Offences	0	3	10
Fraud Act 2006	12	7	7
Proceeds of Crime Act 2002	0	0	16
Total Alternative Convictions	*14*	*11*	*33*
Total Terrorist Financing Convictions (England, Scotland and Wales)	*N/A*	*39*	*47*

Source: Financial Action Task Force, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom – Mutual Evaluation Report', December 2018, p. 96.

Note: There is a discrepancy between the reproduced table in this chapter and the table in the MER. This is due to addition errors in the FATF document.

As Table 2 illustrates, a material number of terrorist financing-related convictions and prosecutions rely on the UK's fraud statutes – for example, in 2015/16, 43% of terrorist financing-related prosecutions and 36% of convictions were fraud related, supporting the observation of one interviewee that 'fraud has proved to be a way of disrupting people where terrorist financing prosecutions are more challenging, particularly when related to associates and facilitators rather than the terrorist actors themselves'.[193] Leading with a fraud charge may also have been an 'easier' means of disruption at a time when the appetite and capacity of the security authorities to monitor subjects of interest was reduced and thus gathering the necessary evidence to press for a terrorist financing charge became more challenging.[194]

193. Author video interview with former UK law enforcement officer, 1 July 2020.
194. Author video interview with former UK financial investigator, 6 July 2020.

This approach to financial disruption may be particularly appropriate in the future where individuals that pose a threat to national security are not part of a proscribed organisation and as the UK national security threat from lone actors and small cells expands to include a greater number of extreme right or single-issue actors. In this landscape, meeting the evidential threshold for terrorist financing prosecutions is likely to be challenging. Thus, a fraud-related charge, as a means of disruption, may be the most effective law enforcement response. As one interviewee noted, '[e]veryone has committed fraud; you just have to look for it'.[195]

Recommendation 12: Emphasis should be placed on ensuring the necessary skills are maintained to ensure fraud investigation remains a key tool in the armoury of counterterrorism policing, with additional training on fraud investigation and prosecution provided where necessary.

Finally, as with all forms of financial crime, the value of the private sector must be harnessed, given the capabilities these institutions already dedicate to anti-fraud activity and the role they inevitably play in efforts to launder the proceeds of any form of fraud. As the UK's JMLIT structure evolves, given the prevalence of fraud in terrorist financing, a dedicated joint working group between the JMLIT Terrorist Financing Expert Working Group and the Joint Fraud Taskforce should be established.

Recommendation 13: The UK's JMLIT Terrorist Financing Working Group and the Joint Fraud Taskforce should establish a new cross-taskforce working group.

In sum, although the financial scale and volume of fraud conducted for terrorist financing purposes is small as a proportion of overall fraud, the result of the financing provided by these frauds can be devastating. It is also clear that whilst these frauds are largely undertaken by lone and small cell actors, many of these actors are looking to the world of organised and volume fraud as inspiration. The methods they use to raise the funds – such as courier and online marketplace frauds – are largely indistinguishable from those used by organised criminals, despite the intentions behind raising the funds being different. In short, fraud in this context further challenges the notion of it being a 'low-harm' crime. Thus, in considering the nexus of fraud and national security, the role of fraud in terrorist financing must be emphasised.

195. *Ibid.*

Conclusions

THE UK'S GROWING fraud problem has wide-reaching impacts beyond the purely financial losses which are frequently the focus of the debate. Perhaps unique to this crime type, fraud has the potential to disrupt society in multiple ways, by psychologically impacting individuals, undermining the viability of businesses, putting pressure on public services, fuelling organised crime and funding terrorism.

Despite growing public and political recognition of the problem, the response to date – which has largely been based on a purely criminal justice-led model and a vastly under-resourced one at that – has failed to turn the tide on a crime type which continues to see year-on-year growth. This paper therefore makes the case for a change in tack.

The financial scale of the problem alone gives cause enough to describe fraud as a national security concern. Yet, the issue continues to receive a lower billing in both the general national security debate and when considering recognised specific national security threats like SOC and terrorism, which in turn translates into lower resourcing and operational prioritisation. This is in part due to its hidden and less media-worthy nature when compared with other national security threats. However, as set out consistently throughout this paper, part of the reason for this can be traced back to a fundamental misrepresentation of fraud as a low-harm crime type, with limited impacts, mainly affecting those on the periphery of society.

This paper challenges these perceptions of fraud by setting out clear examples of the harmful broader impacts it has on society. By doing so, this paper makes the case for a more prominent place for fraud in the national security dialogue. The benefits of moving towards a national security-focused approach are evident: greater leadership, more resources and a 'whole of system' response to the problem. However, while a more prominent role for fraud in the national security dialogue is an important first step, actions – not words – will be key to turning the tide on the 'many-headed' hydra of fraud.[196] This paper points to some clear priorities for attacking fraud as a national security concern:

- There are substantial lacunas in the national understanding of the totality of the fraud problem. Whether through better tasking of intelligence agencies, increased support for academic research or better data-sharing and collaboration between the public and private sectors, gaining a *better strategic understanding* of the ways in which fraud manifests itself as a threat to society, as an organised crime threat or as a funding stream for terrorism will be key to designing a new blueprint for the future response.
- There is a need for *better leadership* in the fraud sphere, both at central government and law enforcement levels, to deal with the 'responsibility vacuum' around fraud. This can

196. Griffin, 'How Fraud Could Destabilise Global Economies'.

be achieved, in part, by establishing a 'whole of system', public–private fraud strategy, with clear reporting lines and responsibilities.

- Fraud continues to be an under-resourced area within policing, the wider public sector and the intelligence community. It is essential that a new fraud strategy comes with a significant boost in resourcing across the system. This includes funding for a new national-to-local law enforcement response, ring-fenced intelligence community resources and further investment in the public sector counter-fraud function. All of this should be bolstered by a new approach to public–private partnership in the fraud response.
- Fraud intersects with other established areas of national security in clear ways, whether that be the cyber, organised crime or terrorism threat. Fraud may be just one facet of these broader issues, but its under-representation as a vector of these issues presents an incomplete picture of the national security threat. While the paper proposes that a specific focus on fraud as a national security concern is needed to shift the dial in the response, it is also essential that in doing so, pathways for *interdisciplinary connections* are built, both in organisational and informational terms.

In short, from whichever angle the problem of fraud is assessed, its continued lack of prominence in the UK's national security dialogue is hard to justify. Conversely, only the focus, leadership and resourcing which a national security response provides will be able to turn the tide on the 'volume crime of our time'.[197]

197. Cifas, 'Fraudscape 2019', p. 11.

About the Authors

Helena Wood is an Associate Fellow of RUSI's Centre for Financial Crime and Security Studies, where her research focuses on implementation of the UK's Economic Crime Plan (2019–22) and the use of asset recovery tools in the fight against serious and organised crime. Prior to establishing her own consultancy business in 2015, Helena worked in the UK public sector and law enforcement with roles at the National Crime Agency, HM Treasury and the Charity Commission.

Tom Keatinge is the Director of the Centre for Financial Crime and Security Studies at RUSI. His research focuses on matters at the intersection of finance and security, including the use of finance as a tool of intelligence and disruption. He has a Master's in Intelligence and International Security from King's College London, where his research focused on the effectiveness of the global counterterror finance regime. Prior to joining RUSI in 2014, he was an investment banker for 20 years at J P Morgan.

Keith Ditcham is Senior Research Fellow and (Acting) Director of RUSI's Organised Crime and Policing team, bringing over 19 years' experience and thematic expertise in serious and organised crime (SOC). He has worked in North, Central and South America and within Europe. His expertise includes counter narcotics and associated money laundering, anti-bribery and corruption investigations, human trafficking, illegal immigration, fraud and firearms trafficking. He possesses a detailed knowledge of the factors which enable SOC, its impact and how it affects specific outcomes.

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.