Occasional Paper

Public–Private Security Cooperation
From Cyber to Financial Crime

Hugo Rosemont
Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK’s leading independent think tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

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

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

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

RUSI Occasional Paper, August 2016. ISSN 2397-0286 (Online).
Contents

Acknowledgements v
Acronyms and Abbreviations vii
Foreword ix
  Tom Keatinge
Executive Summary xi
Introduction 1
I. The Current Landscape 5
II. Introducing the JMLIT 13
III. Introducing CiSP 17
IV. Lessons for the JMLIT 21
V. Conclusion 31
About the Author 33
Acknowledgements

This Occasional Paper would not have been possible without the insights offered so generously by more than a dozen leading security policy practitioners based within government, industry and academia, for which the author is extremely grateful. My particular thanks go to Benedict Wilkinson of King’s College London, for reviewing an early draft of the manuscript, Benoît Gomis and Ewan Lawson, who provided me with enormously valuable feedback, and the Publications team at RUSI. I am also very grateful to Tom Keatinge and especially Inês Sofia de Oliveira, at the Centre for Financial Crime and Security Studies at RUSI, for all their support and for providing me with the opportunity to complete this project. I would like to thank my family on both sides of the Atlantic for their constant encouragement of my work on public–private security cooperation. Above all, I wish to thank my wife, Helen, for her unwavering support of all my efforts.
Acronyms and Abbreviations

BBA  British Bankers’ Association
CERT-UK  UK National Computer Emergency Response Team
CFCS  RUSI’s Centre for Financial Crime and Security Studies
Cifas  Credit Industry Fraud Avoidance System
CISP  Cyber-security Information Sharing Partnership
CNI  Critical National Infrastructure
CPNI  Centre for the Protection of National Infrastructure
CSS  UK Cyber Security Strategy
CSSC  Cross-sector Safety and Security Communications
FSF  Financial Sector Forum
GCHQ  Government Communications Headquarters
IEs  CPNI Information Exchanges
JMLIT  Joint Money Laundering Intelligence Taskforce
NCA  National Crime Agency
NCSC  National Cyber Security Centre
NSRA  National Security Risk Assessment
RISC  UK Security and Resilience Industry Suppliers Community
SDSR 2015  Strategic Defence and Security Review 2015
Over the past two years, there has been considerable focus in the UK on developing a strategic and tactical partnership between the public and private sectors in order to achieve a step-change in the country’s response to financial crime. Speaking at RUSI in June 2014, Theresa May, the then home secretary, emphasised the importance of the partnership between private sector companies and law enforcement to tackling financial crime, preventing money laundering and recovering the proceeds of crime. The result: the formation of the Financial Sector Forum and the creation of the Joint Money Laundering Intelligence Taskforce (JMLIT), a public–private partnership dedicated to collaboration in order to enhance the national response to financial crime.

While this nascent effort appears to be gaining traction, and the JMLIT is being moved to a permanent footing, it is certainly not the first such initiative to be established. This paper from RUSI’s Centre for Financial Crime and Security Studies considers lessons that can be learnt from the establishment of previous public–private partnerships, in particular the Cyber-security Information Sharing Partnership (CiSP). The author stresses the importance of establishing measurable objectives that are co-designed and agreed upon from the outset. Too often such partnerships, established in good faith and with undoubted commitment, fade as the initial enthusiasm wanes, staff are reassigned, and those contributing time and resources question the value of their commitment.

As the UK’s JMLIT emerges from its pilot phase, the longevity of this initiative will be challenged as its initial momentum fades. It is therefore critical that the JMLIT draws on the experience of other, similarly important public–private sector security partnerships in order to anticipate and address the challenges it might face as it matures. It is this process that Hugo Rosemont’s paper seeks to inform.

Tom Keatinge
Director, Centre for Financial Crime and Security Studies, RUSI.
Executive Summary

THIS OCCASIONAL PAPER from RUSI’s Centre for Financial Crime and Security Studies (CFCS) reassesses the importance of public–private engagement on money laundering and cyber security issues, providing new insights into how best to achieve this cooperation. It is designed to offer a set of practical recommendations from a recent, high-profile effort at public–private security cooperation that, if adopted, would help to ensure that the next phase of the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT) initiative is implemented effectively.

Having situated the research in the current UK threat context and in the framework of policy debates on the role of the private sector in national security, and having presented an overview of some of the main forms of public–private security cooperation today, the paper explains the origins of the JMLIT. It then offers new lessons for the taskforce’s development, derived from an in-depth analysis of the UK’s primary existing mechanism for sharing cyber security-related threat information across the public and private sectors: the Cyber-security Information Sharing Partnership (CiSP). Seen by some as a valuable, potentially ‘best practice’ model of operational public–private security coordination, lessons from the CiSP case study are drawn from primary research, including a programme of interviews conducted with UK cyber security practitioners. The paper examines the origins, character and effectiveness of CiSP to show how, while it is a very laudable initiative, its development is not yet optimal or complete.

Against this backdrop, the paper offers three general recommendations for public–private security cooperation that could usefully be applied to the future development of the JMLIT:

Recommendation 1: Any public–private security partnership should establish objectives that are co-designed and agreed on by all relevant stakeholders from the outset. There should be tangible metrics that all parties agree to deliver, monitor and regularly review.

Recommendation 2: To avoid duplication and confusion, proper consideration should be given at the outset to how any proposed public–private security initiative will connect to (if at all), and coordinate with, other existing methods of security cooperation.

Recommendation 3: When designing security-related partnership initiatives, public and private sector stakeholders should devote more time to joint consideration of what each party seeks to gain from the partnership in a practical sense.

The various parties involved with the JMLIT are today presented with an immediate opportunity as a result of the recent decision to extend the pilot project, combined with a growing openness on the part of many authorities to developing stronger public–private security cooperation. Few would now question that, when addressing security risks such as
financial crime and cyber insecurity, public–private cooperation is an essential component of the response. The hard-won, longer-standing experience of CiSP therefore offers useful lessons for the development of the JMLIT, other similar information sharing initiatives, and public–private security cooperation in general.
Introduction

Governments will have to learn how to select and work with private sector collaborators, partly because the latter own most of the critical infrastructure that we must make less vulnerable.¹

Philip Bobbitt.

GOVERNMENT CANNOT ACHIEVE this on its own.’ This observation is often asserted in support of the view that the private sector needs to play a critical role in national security, and it is often echoed in government speeches and policy documents.² In late 2015, the then Chancellor of the Exchequer, George Osborne, explained the UK’s approach to cyber security, for example: ‘This requires effort by all of us – government and industry, start-ups and universities, agencies and allies.’³

This is not a sudden realisation, nor a recent phenomenon. For centuries, private companies have helped states to realise their security objectives: the large-scale use of mercenaries within the Ottomans’ armed forces, for example, or the role played by the East India Company in delivering the British Empire’s economic growth, are just two well-known examples. Yet, in recent decades, governments of modern, liberal market economies, such as the UK, have shown greater awareness of their dependence on private companies to implement their security objectives. Flick through any contemporary security strategy document designed to counter a major contemporary security threat, such as terrorism or organised crime, and reference is quickly made to the multiple, vital contributions of private companies. Whether it is the protective security measures implemented by the operators of the UK’s critical national infrastructure (CNI), such as power stations and airports, the cooperation that has been fostered between internet service providers and the state to remove extremist online material, or the roles and responsibilities of the banks in helping to counter money laundering and other cyber criminality, private sector contributions to national security have become increasingly prominent.

This is particularly true of the arrangements now emerging in the cyber security sector. For example, the UK government’s first cyber security strategy document of 2009 argued that partnership with the private sector ‘will be fundamental’ and that ‘industry and other stakeholders will have a key role to play in the work required to realise the UK’s vision for

---

cyber security.' The most recent edition of the UK’s cyber security strategy (CSS), published in 2011, similarly reasserts the case that: ‘Though the scale of the challenge requires strong national leadership, Government cannot act alone.’ The document is quick to acknowledge that ‘achieving this vision will require everybody, the private sector, individuals and government to work together.’ In presenting the document to Parliament, the government minister then responsible for the strategy elaborated upon the mantra, explaining:

This strategy outlines how we will cement a real and meaningful partnership between the Government and private sector in the fight against cyber attacks, to help improve security, build our reputation as a safe place to do business online, and turn threats into opportunities.

The government’s much-repeated policy, therefore, is that the private sector has an essential role to play in striving for security. As this paper helps to illustrate, though, the extent to which this role has been properly defined is often variable at best; at worst, it can be unclear or ill-thought-through.

Yet there is arguably also a growing recognition that, on security issues ranging from terrorism to financial crime, governmental collaboration with private companies can and must be significantly improved; the statement within the Strategic Defence and Security Review 2015 (SDSR 2015) that the government will ‘work more closely with the private sector and allies to strengthen its contribution to our national security’ is an indication that, at the highest levels of security policymaking in Britain, additional effort is urgently needed on this issue. Against that backdrop, this Occasional Paper will focus on two specific, contemporary structures that have been created to address different problems, this paper seeks to draw conclusions from the experience of the longer-established of the two forums: the Cyber-security Information Sharing Partnership (CiSP), the primary mechanism for information sharing regarding cyber threats. It aims to apply the lessons learnt from the examination of this forum to the future development of the Joint Money Laundering Intelligence Taskforce (JMLIT).

This paper analyses the origins, character and effectiveness of CiSP to inform discussions on how to strengthen the JMLIT. It offers observations on some of the perceived limitations of the

---

partnership approach that has been developed through this mechanism, while recognising that,
overall, it has emerged as a highly constructive and laudable initiative. It shows that while the UK
government and its associated agencies have accepted the principle of working with the private
sector through CiSP, in practice there is still more to do to deliver the agile, fully cooperative
mechanism that most parties agree is needed to facilitate private sector contributions to
cyber security.

A major claim of this Occasional Paper, which all concerned parties in both government and
industry are urged to consider, is that the crucial question is not whether cooperation is
desirable, but how to create optimal methods of cooperation in practice. Conclusions drawn from
the experience of CiSP suggest that the development of better coordinated, and increasingly
well-defined partnerships between the public and private sectors – and whose effects can be
measured – is central to success in any effort at public–private cooperation. It makes the case
for those charged with the development of the JMLIT to heed these lessons as an urgent priority.

This paper is observational: it does not claim to take account of the views of all actors within the
cyber security or financial sectors. However, drawing on original interviews and other sources,
it seeks to offer a selection of constructive ‘lessons learnt’ for the future development of the
JMLIT, and of public–private security cooperation in general.
I. The Current Landscape

Cyber crime is a real and present danger and financial institutions are on the front line.¹

John McFarlane, the chairman of Barclays.

FF THE UK’s economy and national security are linked, as is now frequently acknowledged, it follows that organised criminal activity directed towards – or taking place within – the country’s wealth-creating sectors, such as financial services, is a mainstream national security risk. According to the SDSR 2015, organised crime ‘costs the UK at least £24 billion every year’;² this problem is also judged by the National Security Risk Assessment (NSRA) to be a ‘tier two’ risk to UK national security.³

Within this context, the damage inflicted by money laundering from both a security and economic perspective has been explicitly recognised. The UK National Risk Assessment of Money Laundering and Terrorist Financing, published in October 2015, states that ‘money laundering represents a significant threat to the UK’s national security’,⁴ citing UN figures to conclude that ‘The best available international estimate of amounts laundered globally would be equivalent to some 2.7% of global GDP or US$1.6 trillion in 2009.’⁵ While the use of offshore structures can be entirely legal, seemingly credible allegations of large-scale criminality arising from the swathes of recently leaked client data belonging to the law firm Mossack Fonseca – the so-called ‘Panama Papers’ – also indicate the scale of the potential illegalities.⁶

The extent to which this form of criminality afflicts the British banking sector is difficult to measure, yet there is no question in general terms about its considerable size and seriousness. The government has concluded that, together with terrorist financing, money laundering serves to:

- undermine the integrity of our financial institutions and markets, enable criminals to hide, store and benefit from the proceeds of their crime, and enable terrorist groups to function, recruit and commit terrorist acts. Money laundering into and through the UK financial system is also related to grand corruption overseas – the bribery and theft of public funds.⁷

---

². SDSR 2015, p. 17.
³. Ibid., p. 87.
⁵. Ibid., p. 3.
There is equally no doubt that, given the importance of the City of London as a global financial hub, the UK has a central role to play in mitigating the problem. As the SDSR 2015 explicitly states, ‘substantial funds from crime conducted around the world are laundered through London’.8

Of course, money laundering is only one of many threats currently facing the UK financial sector. The seriousness with which the government assesses the impact of cyber attacks on both the sector and the wider economy has been made clear in the SDSR 2015. The NSRA has stated that cyber security is a ‘tier one’ threat – one of the six highest priority security risks facing the country – and significant new resources have been made available to counter the challenge.9

Setting out the severity of the problem, the SDSR 2015 recognised the diversity of the internet-based or -enabled threats facing the UK today:

The cyber threats to the UK are significant and varied. They include cyber terrorism, fraud and serious and organised crime, espionage, and disruption of CNI [Critical National Infrastructure] as it becomes more networked and dependent on technology, including networks and data held overseas.10

It is important to understand the multifaceted character of cyber threats facing the UK in order to formulate an appropriately nuanced response to them in all their diversity. It also helps to explain why such a large number of government departments, agencies and sectors – including the banking community – are all involved in the pursuit of more robust cyber security.

Cyber or ‘e-crime’ is now clearly recognised as a major threat to both the UK economy and national security: the SDSR 2015 sees it as one of the ‘most significant types’ of serious and organised crime.11 It is fair to say, however, that the true cost of cybercrime continues to elude both analysts and policymakers. One analyst notes that ‘the scale of such crime in the UK and its cost to the economy have proved challenging to quantify’,12 and the National Crime Agency (NCA) has also acknowledged that it ‘is unclear at present.’13 The difficulties associated with achieving an accurate assessment are widely recognised,14 and were made apparent in the publication of a jointly badged Cabinet Office/Detica report of February 2011, which estimated

---

8. SDSR 2015, p. 17.
9. The SDSR 2015 states that the government ‘will invest £1.9 billion over the next five years in protecting the UK from cyber attack and developing our sovereign capabilities in cyber space.’ Ibid., p. 40, para. 4.105.
10. Ibid., p. 85.
11. Ibid., p. 18, para. 3.14.
that cybercrime costs the UK £27 billion annually.\textsuperscript{15} Reaction to the report was broadly critical and one study noted that it ‘was greeted with widespread scepticism and seen as an attempt to talk up the threat’\textsuperscript{16} while also questioning its methodological rigour. Such is the difficulty in reaching an agreed-upon, reliable figure of the harm inflicted by cybercrime that the National Audit Office hedged its bets in concluding that ‘cybercrime currently costs the UK somewhere between £18 billion and £27 billion a year.’\textsuperscript{17}

Other sources help to indicate the size of the problem. Recent remarks by Robert Hannigan, the director of the UK government’s signals intelligence agency, the Government Communications Headquarters (GCHQ), do not paint a rosy picture. Hannigan referred to ‘the industrial-scale theft of intellectual property from our companies and universities’;\textsuperscript{18} the then home secretary, Theresa May, made a similar point when, considering the impact of digital crime, she referred to the ‘industrial scale fraud we now see committed over the internet.’\textsuperscript{19} Within business, there is also growing recognition that cybercrime constitutes a major threat to the economy, as noted by leading industry trade associations. According to statistics cited by the British Bankers’ Association (BBA), for example, ‘More than 70 per cent of banking and capital market CEOs identify cyber insecurity as a threat to their growth prospects.’\textsuperscript{20} Similarly, the British Retail Consortium’s Retail Crime Survey in 2014 highlighted that ‘The majority of retailers said cyber attacks remained a critical threat to their business.’\textsuperscript{21}

If the scale of the security challenges facing UK businesses is now being recognised, how should these challenges be addressed? As noted above, the UK government’s judgement is that public–private cooperation should be an essential component of the response to such threats. Before considering two specific mechanisms designed to improve public–private cooperation, this paper briefly outlines the broader debates that emerged during the course of the author’s research into the private sector’s involvement in contemporary national security.


\textsuperscript{18} Robert Hannigan, ‘Front Doors and Strong Locks: Encryption, Privacy and Intelligence Gathering in the Digital Era’, speech made by the director of GCHQ to the Massachusetts Institute of Technology, 7 March 2016.


The Character of UK Public–Private Security Cooperation Today

Extensive Private Sector Involvement in Security

It is important to recognise that private companies have long been involved in, and are now arguably central to, the implementation of many strands of contemporary UK national security strategy. For several decades, inquiry into the character, effectiveness and appropriateness of private sector involvement in the security sector has clearly illustrated extensive industry contributions to the national defence sector, including the activities of private military and security companies operating overseas.

Yet, today, it seems that not all senior policymakers fully appreciate the extent of private sector involvement in the national security sector. While it has long been recognised that 85% of the UK’s CNI is owned by the private sector, the operation of the mechanisms established to ensure its security is less well documented. It is now necessary to adopt a broader and deeper understanding of private sector security involvement; private managers of airports and power stations are arguably as much contributors to national security as they are providers of essential services.

There are numerous examples of how the private sector has become deeply involved in providing security against diverse, complex and often transnational security risks. It has fulfilled large-scale contracts in areas such as border security, emergency preparedness and Olympic security, among others; indeed, since 9/11, the UK government has funded security contracts to the tune of billions of pounds. There is also evidence of other less formal arrangements being established to strengthen public–private cooperation on security issues. The UK Security and Resilience Industry Suppliers Community (RISC), for example, has been created as a main channel of communication between the government and industry on matters of national security – a policy-level public–private partnership – and undertakes a varied portfolio of activity to support the government’s counterterrorism objectives, including efforts to strengthen technological innovation and facilitate consultation during emergency situations. At the operational level, there has been a proliferation of partnerships; the Cross-sector Safety and Security Communications (CSSC) initiative, for example, has been rolled out across several sectors as a particularly successful ‘platform to facilitate communications between private and public sector on issues surrounding security and business resilience.’

known, it seems that few areas of national security strategy are now considered ‘off limits’ for privatisation. Indeed, such is the reported extent of outsourcing in the US intelligence field that one analyst has suggested that we may be witnessing the emergence of an ‘intelligence-industrial complex’.

It is one thing to list or describe the diverse, proliferating range of public–private partnership initiatives that have been emerging in the UK security sector, it is quite another to assess how they should be structured and operate. This is not a straightforward task – arguably, the concept of what constitutes an effective ‘partnership’ has not attracted the theoretical and policy attention it deserves. While some work has been conducted in this field, policymakers have not yet fully appreciated the ‘multiplicity of roles’ that companies play, or could play, in UK national security. With only a few exceptions, conceptual frameworks for analysing the spectrum and significance of private sector involvement in security are underdeveloped.

This shortcoming was addressed recently by Madeline Carr, senior lecturer in International Relations at Cardiff University, who, examining the character of public–private partnerships in delivering national cyber security strategies, argued that ‘there is a fundamental disjuncture between the expectations of the two partners in terms of roles, responsibility and authority.’ It would be worrying if Carr were correct in her contention that the model of ‘partnership’ outlined in current policy documents is ‘deeply flawed’ as she recognises, such partnerships are central to the UK’s current cyber security approach. While agreeing with many of Carr’s points, this Occasional Paper will seek to temper her pessimism by offering lessons that, if acted upon, could help to foster the kind of partnership she suggests may be unworkable. Among existing efforts to address financial crime and cyber insecurity more generally, there is already much evidence to suggest that companies are willing to cooperate where there is mutual benefit in doing so. The trick will be to ensure that hard-won best practices developed from past experience are fully applied to emerging initiatives such as the JMLIT.

Information Sharing Partnerships

How is public–private security cooperation evolving in the digital context? Insofar as the partnerships designed to counter money laundering and strive for cyber security are concerned, it is safe to say that the identification by different departments of the need for public–private cooperation has resulted in a growing proliferation of initiatives. Numerous government departments and agencies have started to develop methods of collaborating with companies in the field of contemporary security policy, many of which provide vital access to digital networks, data and general situational awareness. As these relationships have developed they have evolved into multiple, more structured partnership initiatives.

In the sections that follow, this paper considers two of the UK’s main security-related information sharing mechanisms today, the JMLIT and CiSP. While, as indicated above, information sharing mechanisms are only one form of public–private security partnership, they are, at least at present, a popular, prominent and wholly workable mechanism for furthering cooperation. The JMLIT and CiSP are not the only mechanisms for sharing operational data with the private sector on security issues. Among others, prominent initiatives include the fourteen ‘information exchanges’ (IEs) hosted by the Centre for the Protection of National Infrastructure (CPNI), designed to enable the sharing of sensitive data between individual sectors of the CNI. Despite the sensitivity of their activities, the rationale for the IEs has been explained:

Sharing of information about the risks facing networks is beneficial to both government and industry. CPNI facilitates ‘information exchanges’ which allow one company to learn from the experiences, mistakes and successes of another, without fear of exposing company sensitivities.32

A similar initiative is also operated by GCHQ, which in 2014 announced that it would ‘be working with security-cleared personnel in trusted service providers to enable them to become the UK’s first line of defence in countering cyber threats to the nation’.33 As only limited details of the scheme are publicly available, it is hard to determine whether it connects to the work of other information sharing schemes already underway. GCHQ was notably insistent, however, in expressing that it would ‘complement, not replace, some excellent threat intelligence that is already available from industry and government’, including specifically via CiSP.34

While one recent report has helpfully ‘mapped out’ the information sharing landscape for cyber security as it relates to the finance sector,35 generally, the picture that emerges is one of proliferating, sometimes overlapping and not fully coordinated instances of public–private cooperation on security issues. As the following pages will show, doubts have been raised

34. Ibid.
35. TheCityUK and Marsh, ‘Cyber and the City’, p. 21.
in this unsettled context about how far partnership really extends between the public and private sectors on security matters. Though the diversity of the landscape and multiplicity of actors certainly present challenges, it would also appear that the government and industry both recognise that the time has come for stronger cooperation and better coordination of the various public–private initiatives that have been designed to address financial crime and cyber security. The following sections illustrate how this has begun to be addressed through the JMLIT and CiSP.
II. Introducing the JMLIT

The scale and complexity of serious and organized crime, including financial crime such as money laundering, requires more than just a law enforcement response. It requires active partnership between government and industry.¹

Theresa May, then Home Secretary, February 2015.

Whether as a result of the security or economic effects of financial crime, or a combination of both, public–private cooperation has evolved into a central component of the UK’s policy response to serious organised crime. As with other areas of national security policy, government agencies have come to appreciate that they are highly reliant on the private sector. For example, in the case of financial crime such as money laundering, government agencies have a high level of dependency on the banks. Whether through the tool of regulation or more preventative initiatives, state agencies have sought to cooperate with the banking sector, and a clear appreciation has developed that such cooperation is essential to achieving the UK’s national security objectives.

While there is no question about the serious level of ambition to address the problem of money laundering more proactively in the UK, it remains open to debate how ‘active’ this and other public–private security partnerships have truly become. A main strand of activity in this respect has been through information sharing between the public and private sectors, as emphasised in a recent article by Tom Keatinge, the director of the CFCS.² Recognising that it is through the financial sector’s own networks and systems that information passes, and that this is where the potential for criminality occurs, law enforcement and other agencies have had no choice but to seek to work with the financial sector. However, although such cooperation is needed, the extent to which all elements of the state and the private sector are aware of their mutual dependence, let alone willing to accept it, is not yet immediately apparent. Research conducted for this paper indicates that there is still much work to do to ensure that a proper conversation takes place on what ‘partnership’ in security terms means to the two sides.

Nevertheless, in recent years there has, quite rightly, been a new emphasis on establishing stronger, more formal mechanisms to facilitate information sharing between the public and private sectors to tackle financial crime. The establishment in 2014 of the Financial Sector Forum (FSF), jointly chaired by government and industry, was pivotal in this respect, representing what

the then director general of the NCA, Keith Bristow, described as a ‘unique development’. Bristow candidly outlined in January 2015 both the aim of this new strategic structure and the challenging context in which it had been set up:

The Forum’s aim is to improve information sharing to tackle some of the most damaging and hardest to reach criminals operating in the UK. I don’t think it is unfair to say that, historically, there has been a degree of mistrust between law enforcement, regulators and the financial sector, so it is a tribute to all those involved that this progress has been achieved.

A new premium had clearly been placed on strengthening the previously limited amount of cooperation with the banks, and the focus quickly turned to how to achieve this aim through the development of pragmatic, operational structures. A pivotal moment came in February 2015 with the launch of the JMLIT, an initiative seen as a ‘key achievement’ of the FSF. During a speech shortly before this event, the then home secretary carefully articulated the need for better information sharing:

for too long there has been mistrust between law enforcement agencies and the banks. Information that each party held, which could help root out and stop money launderers and other criminals from causing untold damage, was kept in silos. Everyone – the banks, regulators and law enforcement agencies – realise how short-sighted and unsustainable this is.

This was arguably the birth of what historians may come to see as a new era of security cooperation with UK-based banks. Certainly, it marked the point at which energy was injected into a renewed focus on information sharing between the public and private sectors in order to mitigate the effects of money laundering.

Aims and Key Characteristics

The aim of the JMLIT is well documented: simply put, its purpose is ‘to improve intelligence sharing arrangements to aid the fight against money laundering’. The press release announcing its launch in February 2015 broke down this objective to a more granular level of detail:

The JMLIT has been developed to provide an environment in which the financial sector and law enforcement agencies can exchange and analyse information and intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the UK.

4. Ibid., p.6.
8. Ibid.
The NCA’s website lists the JMLIT as having four specific operational priorities:

1. Understanding and disrupting the funding flows linked to bribery and corruption.
2. Understanding and disrupting trade-based money laundering.
3. Understanding and disrupting the funding flows linked to organised immigration crime and human trafficking.
4. Understanding key terrorist financing methodologies (led by the National Terrorist Financial Investigation Unit in the Metropolitan Police Service).  

Thus the emphasis of the JMLIT has been to establish an effective operational information sharing mechanism, building on the previous, arguably strategic work of the FSF from which it flowed.

The collaborative manner in which the JMLIT was to achieve its aim was highly innovative, if not unprecedented. Initially planned only as a twelve-month pilot project, it is striking how, from the beginning, it was conceived as a fully inclusive, multi-stakeholder initiative, comprising multiple government agencies, banks and other organisations. The numerous entities involved in the initiative are listed in Table 1 below.

<table>
<thead>
<tr>
<th>Government/Law Enforcement</th>
<th>Banks</th>
<th>Other Organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Office</td>
<td>20 major UK and international banks, including: Barclays; Santander; Standard Chartered; RBS; HSBC; BNP Paribas; Citigroup; Nationwide; Lloyds</td>
<td>British Bankers’ Association</td>
</tr>
<tr>
<td>National Crime Agency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>City of London Police</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Conduct Authority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HM Revenue and Customs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Home Office et al., ‘Anti-money Laundering Taskforce Unveiled’, 25 February 2015; and NCA, ‘Joint Money Laundering Intelligence Taskforce (JMLIT)’.

Drawing on the participation of these multiple contributors, the early evidence suggests that the JMLIT has been of considerable benefit to the UK’s anti-money laundering efforts. According to the government’s new Action Plan for Anti-money Laundering and Counter-Terrorist Finance, for example, the pilot programme ‘has directly contributed to law enforcement operations.

---

including eleven arrests and restraint of £558,144 of criminal funds', as well as identifying ‘Over 1,700 bank accounts linked to suspected criminal activity.¹⁰

A full analysis of the JMLIT’s effectiveness during its short history is outside the scope of this paper; as stated above, the aim is to formulate a set of lessons for the next phase of the initiative from another, longer-standing public–private partnership, CiSP. Before turning to that project, however, it is important to record that such is the perceived success of the JMLIT initiative to date, the decision has been taken to extend the life of the project and 'put the taskforce on a permanent footing’ by July 2016.¹¹

This is not to suggest that there is somehow little or no room for improvement. On the contrary, Clare Ellis and Inês Sofia de Oliveira have highlighted that, while it constitutes a success, the JMLIT was only initially designed as ‘a limited pilot programme operating in relation to individual cases and including only certain banks.’¹² Thus, particularly in the context of the government’s ambition to deliver an expansion of the JMLIT,¹³ its planned continuation offers an opportunity to consider how it could be developed most effectively.

Cyber Security Information Sharing Partnership is a joint, collaborative initiative between industry and government to share cyber threat and vulnerability information to increase overall situational awareness of the cyber threat and therefore identify the risks to reduce the impact upon UK business.¹


In launching CiSP in March 2013, the then minister for cyber security, Francis Maude, explained the rationale for partnership and information sharing between the public and private sectors: ‘by building a community of public and private partners, we could all pool our information on cyber threats and increase our visibility of cyber threats for mutual benefit’.²

The potential security benefits gained by sharing threat data were reiterated by government officials and industry executives operating in the UK cyber security sector in interviews conducted for this Occasional Paper. One participant stressed, for example, that ‘information sharing is crucial for cyber security’,³ while another, contemplating how to generate optimal public–private cooperation, argued that ‘most of [the] options come back to data sharing.’⁴ While it is also apparent that (as with any cyber security initiative) sharing information between the public and private sectors could never be a ‘silver bullet’⁵ – a more nuanced, comprehensive approach is needed – it has emerged as possibly the key element of cooperation.⁶ The primary mechanism for achieving this in the UK is CiSP.

Plans to develop a new mechanism for information sharing within the UK cyber security sector came to fruition on 14 February 2011, when the then prime minister, David Cameron, held a ‘tea party’ at 10 Downing Street with ‘the heads of some of the largest companies from all sectors of the UK economy to discuss the cyber threat and our shared interest in getting the response right.’⁷ Dubbed as the ‘Valentine’s Day meeting’, senior representatives of companies including British Airways,
Centrica, National Grid and BT were in attendance.\(^8\) This meeting is seen within government as a key moment in the development of CiSP; according to the then minister for cyber security, this was when ‘we started to tackle this issue’.

Minutes of the meeting are not publicly available; however, statements at the time indicate how 10 Downing Street looked upon the need for partnership on cyber security issues. According to one record:

> Asked if the Prime Minister was speaking to companies to gain their experiences or to warn them, the PMS [prime minister’s spokesman] said both. It was something that companies had to think about themselves – how they protected their systems. It was also an issue that the Government thought could be better tackled if we worked together.\(^9\)

It is the author’s contention that while 10 Downing Street saw potential for ‘working together’ in strengthening cyber protection, the government also believed that a large – if not the largest – part of the response would need to come from the private sector itself, seemingly on terms that the former would set out. The extent to which this laid the appropriate foundations for the development of a genuine partnership will be examined later in the paper.

The meeting at 10 Downing Street led to the initiation of ‘Project Auburn’, the direct predecessor of CiSP, which, not dissimilarly to the JMLIT, was described as a ‘pilot of a joint public/private sector cyber security “hub”’ that was designed ‘to promote information sharing between government and industry on attacks and potential threats.’\(^10\) Further details about the ‘hub’ were provided in the government’s Cyber Security Strategy (CSS) of 2011, published at around the same time:

> A joint public/private sector ‘hub’ will pool government and private threat information and pass that out to ‘nodes’ in key business sectors, helping them identify what needs to be done and providing a framework for sharing best practice.\(^12\)

According to the CSS, the pilot would at first involve five sectors: defence; finance; telecommunications; pharmaceuticals; and energy.\(^13\) Data also indicate that Project Auburn initially involved around 80 companies, extending to 160 by the time it became the CiSP.\(^14\) While the director


\(^9\) Maude, ‘Cyber Security Information Sharing Partnership’.

\(^10\) ‘Number 10 Press Briefing’.


\(^12\) Cabinet Office, ‘The UK Cyber Security Strategy’, p. 28.

\(^13\) ibid.

\(^14\) Maude, ‘Cyber Security Information Sharing Partnership’.
of the UK National Computer Emergency Response Team (CERT-UK) later called the pilot ‘clunky’, at the time it was under development the government persevered and maintained an ambition to extend the benefits of information sharing to the business community more broadly. It launched CiSP formally at Chatham House in March 2013.

**Aims and Key Characteristics**

What did CiSP set out to achieve and how does it operate in practice? As indicated above, its main aim was to build across government and industry – by way of an online mechanism through which operational data could be voluntarily shared – an initiative that generated stronger situational awareness of the cyber security threats affecting the UK than had previously been the case. In general terms, the ambition of CiSP was to:

- give government and industry a far richer, more immediate intelligence picture of the cyber threat.
- For the first time a new secure, virtual collaborative environment will allow government, including the Security Service, GCHQ and the National Crime Agency, and industry partners to exchange information on threats and vulnerabilities as they’re identified.

This central aim has been repeatedly highlighted by government officials from CERT-UK, established in March 2014 and subsequently tasked with responsibility for CiSP. According to Chris Gibson, the director of CERT-UK, partnership is central to his organisation’s activity because: ‘Our aim is to build trust, foster collaboration, and encourage the sharing of information to develop the situational awareness we need to support our cyber security objectives.’

For Gibson, ‘cyberspace is simply too big for any one organisation – whether public or private sector – to have sight of everything that is occurring.’ By combining resources, therefore, it is believed that the public and private sectors can help to strengthen each other’s security. Supporting this vision, many prominent public and private organisations are listed as ‘partners’ on the official CiSP website.

In practical terms, CiSP is ‘a jive-based social networking platform’, hosted on the internet, which ‘allows members from across sectors and organisations to exchange cyber threat information in real time, in a secure and dynamic environment, while operating within a framework that protects the

---

18. *Ibid*.
19. The listed members are: Babcock; BAE Systems; BT; EE; FireEye; Lloyds Banking Group; Microsoft; Palantir; QinetiQ; Virgin Media; techUK; KPMG; and Fujitsu.
confidentiality of shared information. According to details of the initiative published by one of the companies involved in developing the platform, CiSP is ‘a secure collaboration environment for cyber incidents’ that allows companies and the government to share data in confidence and, where necessary, in anonymity. According to CERT-UK, registered members of CiSP are provided with free, ‘regular advice and guidance on a range of cyber issues’, including alerts, advisories and best practice guidance. Its website also suggests that an additional benefit of membership is ‘access to privileged information from our international partners and invitations to attend intelligence briefs.’

Central to the operation of CiSP is the stated ability for individual sectors and communities to establish ‘rooms’ on the platform, designed for certain constituencies, which have the ability to control who can access their data. As Gibson correctly notes, ‘people will not share with 3,300 people who they don’t know.’ With this in mind, the platform enables more selective, tailored sharing.

Also vital to CiSP is its overarching ‘Fusion Cell’, a joint public–private, co-located team of analysts. CERT-UK’s official website explains its purpose:

> The Fusion Cell, consisting of government and industry analysts, provides a catalogue of products and bespoke services to its members for free. The team monitors CiSP, examines multiple open and closed sources of information, conducts analysis and as a result can feed back enriched cyber threat and vulnerability information to the CiSP community.

Membership of the Fusion Cell comprises seconded individuals from a variety of organisations, many of whom are said to work for one or two days a week on the initiative. According to the director of CERT-UK, the Fusion Cell adds value because it ‘can see the whole piece’, and thus has the ability to identify threats from anywhere on the platform. In theory, this empowers it to determine whether to deliver advice to the community more broadly if, for example, it believes a particular threat to have wider implications.

24. CERT-UK, ‘Cyber-Security Information Sharing Partnership (CiSP)’.
26. CERT-UK, ‘Cyber-Security Information Sharing Partnership (CiSP)’.
27. Interview with industry executive, by telephone, 17 February 2016; author interview with industry executive, by telephone, 10 March 2016. Chris Gibson presented a list of the members of the CiSP Fusion Cell to a conference in December 2015. It included: Microsoft; Security Service (MIS); BAE Systems; Ministry of Defence; EE, QinetiQ; GCHQ; National Crime Agency; Trend Micro; National Grid; BT, Virgin Media; Babcock; Lloyds Banking Group; City of London Police; Palantir; and Digital Shadows. Gibson, ‘Enhancing Cyber Resilience’, p.17, presentation slides, <http://www.grc-summit.com/europe/2015/downloads/Presentations/Enhancing_cyber_resilience_Chris%20Gibson_CERT.pdf>, accessed 27 March 2016.
IV. Lessons for the JMLIT

if anyone in the room has ideas of more we could do to engage industry then I would be really happy and pleased to hear them.¹


THE UK’S ARRANGEMENTS for public–private cooperation on cyber security issues have been called ‘world leading’ in their field. According to a report compiled for the Department for Business, Innovation and Skills in 2013, for example, ‘The UK rates as above average in international comparisons in its relationships between public and private organisations’; CiSP is specifically listed as one of the ‘instantiations of this’.² Certainly, the government has been keen to promote CiSP as a highly effective initiative for public–private information sharing: upon his appointment as the director of CERT-UK, Chris Gibson referred to CiSP as a ‘powerhouse’,³ and GCHQ has stated that it has provided ‘some excellent threat intelligence’.⁴

There are numerous practical examples of the enormous value of CiSP. In 2014, according to the then minister for cyber security, members of CiSP were informed each day of ‘215,000 abused IP addresses, so they [could] be blocked or dealt with.’⁵ CiSP was also ‘heavily used’ during a major exercise on cyber threats conducted by the financial services sector known as ‘Waking Shark II’. The ensuing report highlighted ‘the value of the facility in identifying and responding to a cyber-event’.⁶ Perhaps more importantly, CiSP has helped to mitigate actual, specific threats. For example, it was directly involved in tackling the ‘Heartbleed’ vulnerability which enabled the theft of data from devices hosting the open-source software library OpenSSL, and which was identified in the first half of 2014: ‘CiSP rapidly warned members of the threat, providing signatures that could be used to detect abuse.’⁷ According to the ‘testimonies’ section on the

⁴. GCHQ, ‘GCHQ Announces New Initiative to Enhance the Protection of the UK in Cyberspace’.
⁷. Maude, ‘Francis Maude Speech at IA14’.
CERT-UK website, the reaction of a ‘large UK based transport organisation’ to CiSP’s handling of ‘Heartbleed’ was as follows:

CiSP detailed actionable and credible information that we used to support our infrastructure. The first 24 hours were crucial in understanding what Heartbleed meant to us. Getting the word out to our suppliers, beginning our analysis and remediation efforts were strengthened by the specific information we received from CiSP.\(^8\)

One of the initiative’s leading original partners, BT, has similarly been cited as being pleased with the support provided by CiSP in relation to Heartbleed: ‘CiSP provided a haven where members could cut through the noise and exchange meaningful updates and intelligence with each other’.\(^9\) As the UK government’s primary mechanism for public–private cyber threat information sharing, there is clear evidence that CiSP has added considerable value to both government and industry.

Nevertheless, a picture of suboptimal public–private partnership relating to CiSP was also presented by interviewees for this study. One industry executive characterised the situation as a ‘parent-child relationship’ where ‘both sides act as a parent’, before suggesting that both could at times be guilty of saying to the other: ‘Thou shalt do!’\(^10\) Another concurred, using the same ‘parent–child’ terminology and asserting that government agencies seek to ‘tell industry what to do’, adding that there is ‘a tendency for the relationship to be skewed both ways.’\(^11\) Another participant stressed that the ‘absolutely most important thing is [that] it is a two-way street’, before suggesting that ‘sometimes it can be a one-way street of private giving and public taking.’\(^12\)

Not all interviewees were as critical: one stated simply that, overall, the government and industry ‘could use each other better’ in the cyber security arena.\(^13\) However, perspectives offered both publicly and privately for this Occasional Paper suggest that, in its current form, CiSP does not operate as effectively as some practitioners believe it could. Attention was recently drawn to the potential flaws of the UK’s overall approach when it was reported that a senior director of GCHQ, Alex Dewdney, delivered a stark assessment of the emphasis that had been placed on such forms of cooperation to date:

---

8. CERT-UK, ‘Cyber-security Information Sharing Partnership (CiSP)’.
9. Maude, ‘Francis Maude Speech at IA14’.
10. Author interview with industry executive, by telephone, 18 March 2016.
11. Author interview with industry executive, Surrey, 24 February 2016.
12. Author interview with industry executive, by telephone, 10 March 2016. The ‘significant concern that information sharing is a one-way relationship’ has also been raised in a US context. See Germano, ‘Cyber Security Partnerships’, p. 3.
there’s been something of a mantra in the UK that the solution to all of our problems is information sharing and public/private partnerships – that if we keep doing that then somehow it will magically cause improvement to happen. That approach by itself is not sufficient.\(^{14}\)

While few (if any) would claim that information sharing or CiSP itself could on their own solve all of the UK’s cyber security problems – or, for that matter, that the JMLIT could counter all financial crime – considerable emphasis has nevertheless been placed on this approach as a central component of the CSS. However, there was scepticism among many interviewees that the CiSP as yet represents an optimal method of cooperation.

One criticism of CiSP is that appropriate metrics – in other words, reliable methods for measuring the effectiveness of an initiative – have not yet been designed nor implemented. In short, there is a perception that, from the government’s perspective, success is gauged by the number of companies that sign up to the platform. Indeed, the growth in the number of participants signing up to CiSP appears to be the key way that its progress is measured. A recent presentation by the director of CERT-UK, Chris Gibson, detailed the logic underpinning this focus: ‘the more members we have on board, the more information that is shared, the better our situational awareness, and the greater our collective resilience.’\(^{15}\) While the ambition to increase membership is well intentioned and an understandable aspiration on the part of the government, it appears that the current emphasis on increasing company numbers may be breeding some cynicism within the private sector: one interviewee referred to this as a ‘pointless metric’,\(^{16}\) suggesting that the government is not sufficiently concerned with other key issues, such as the quality of outputs arising from the cooperation.\(^{17}\) Even in a scenario in which membership of CiSP continues to grow, it is important to recognise the problem, noted above, that not all companies may wish to share sensitive data across the platform. Benefits could therefore be gained from incentivising the cooperation of smaller clusters of participants, perhaps on a sectoral basis. Although there has been some progress in this respect, a view is also emerging that new metrics should be developed for CiSP.

In addition to criticism of a so-called ‘numbers game’ mentality, questions have emerged about the comprehensiveness of CiSP’s coverage. A former government security minister and the first UK special representative to business on cyber security, Baroness Pauline Neville-Jones, has previously called attention to this in an online interview. Discussing the importance of implementing cyber security ‘at scale’, she cautioned about the emphasis on working primarily with big companies: ‘But, you know, the top league is only the top league. And the economy is


\(^{15}\) Gibson, ‘Partnership with Industry’. A similar argument appeared in the speech made by the minister for cyber security at the launch of CiSP: ‘The more volume, the more traffic there is – the more useful it will be to all of us. The more information each member makes available to the community – the richer our collective knowledge.’ Maude, ‘Cyber Security Information Sharing Partnership’.

\(^{16}\) Author interview with industry executive, Surrey, 24 February 2016.

\(^{17}\) *Ibid.*
Public–Private Security Cooperation

actually composed of … this vast number of companies underneath … who also need … to be aware and have some protection’.18

Conversely, in an interview for this paper, one government official was adamant that ‘those companies that matter are in CiSP’.19 In the absence of more information in the public domain about the current membership of the initiative, it has not been possible to validate this assertion.

Separately, concerns were expressed over the extent to which many companies involved in CiSP actively contribute to the initiative, or whether some fall short of fully endorsing the spirit of partnership that it strives for. Several interviewees advanced the idea, for example, that many companies do not contribute at all, in effect behaving as ‘active listeners’20 or, worse, freeloaders; one participant even claimed that ‘half the people have never contributed squat’.21 Data is not publicly available about the proportion of CiSP members who actively contribute to the platform, and absent this, it is not possible to state with confidence what percentage of CiSP members may or may not be willing (or able) to share data on the platform. That said, one government official stated privately that there are at least three main categories of user on CiSP: those who ‘feel comfortable in being proactive’ in sharing; those who just comment upon posts and threads on the platform; and those who are happier simply ‘taking’ information.22 While this is a helpful acknowledgement, greater transparency around the types of members of CiSP, and their behaviours, might help all those concerned – not least policymakers – to draw more meaningful conclusions as to its current effectiveness.

Even more useful, perhaps, is a more general appreciation of the many possible reasons why both government agencies and private sector companies may be reticent to share information on CiSP.23 These emerged during the numerous interviews conducted during the course of the research for this paper. For example, it appears to be an open secret that, as one interviewee put it, ‘companies are wary of sharing sensitive information within [the] portal.’24 The commercial pressures that exist among companies are a significant factor; ultimately, as the same participant noted, ‘they are competitors’.25 One industry interviewee echoed this view, adding that the private sector ‘does share information but at the end of the day we are competitors’, and arguing that companies will be disposed to share only when ‘it doesn’t cause commercial problems’.26 This appears to be a very real, potentially fundamental obstacle to deep partnership

19. Author interview with government official, by telephone, 4 March 2016.
21. Author interview with industry executive, by telephone, 10 March 2016.
22. Author interview with government officials, by telephone, 16 March 2016.
25. Ibid.
26. Author interview with industry executive, by telephone, 10 March 2016.
among companies, added to which is the alleged hesitancy of some government departments and agencies to share information on CiSP, often for separate security reasons. Noting that ‘classification is always a challenge’, the director of CERT-UK has stated his organisation’s desire to share as much sensitive government data with companies as is practical: ‘wherever possible, we go back to people who tell us stuff internally and say: how can I get this to the people who need it?”

It could also be argued that, with the dawn of initiatives such as CiSP and the JMLIT, we are only just entering a new era of more intensive public–private information sharing on security issues. Given the long, mixed record of effective intelligence sharing between even closely partnered, like-minded governments – a collaboration which is still far from optimal – it is little wonder that the UK has encountered several challenges in fostering effective public–private cooperation at such an early stage.

Further illustrating this apparent reluctance to share information, two interviewees suggested that, at the outset of the initiative, the government was only willing to share ‘very little information’ through CiSP. While this was said to have subsequently improved as organisations including the Ministry of Defence and GCHQ seconded officials into the Fusion Cell, one interviewee noted that the initiative had ‘grown out of a culture of secrecy’. Another interviewee summarised that public–private sector information sharing is bedevilled by ‘misconceptions around sensitivity’, on the one hand, and a ‘misunderstanding about what the private sector might share between themselves’ on the other. Reflecting on these difficulties, perhaps it is easy to see why, from the government’s perspective, the issue of getting members to participate in CiSP is recognised to be, as one official put it, ‘without a doubt our biggest challenge’.

Finally, the differing levels of maturity of existing mechanisms for information sharing within individual sectors was identified as a major issue. Space does not allow for a thorough treatment here of the well-documented problem of coordination associated with governmental cyber security policy and operations; for present purposes it is sufficient to highlight the perceived ‘newness’ within security policymaking circles of the cyber threats facing the UK, and of the structures designed to deal with them. Initiatives in this area are very much still seen as ‘works in progress’, subject to constant review, development and reform. Indeed, the seemingly unsettled, cluttered landscape of cyber security-related organisations, activities and initiatives led to the famous assertion by former Chancellor of the Exchequer George Osborne, referenced in one interview for this paper, that there is an ‘alphabet soup’ of organisations and activity in UK cyber security.

In short, a clear consensus has arisen that more needs to be done urgently to coordinate the various cyber security initiatives, and the private sector’s contributions to them, more effectively.

27. Gibson, ‘Enhancing Cyber Resilience’.
28. Author interview with industry executive, by telephone, 10 March 2016. This point was echoed in author interview with industry executive, London, 15 February 2016.
31. Author interview with government officials, by telephone, 16 March 2016.
33. Osborne, ‘Chancellor’s Speech to GCHQ on Cyber Security’.
It may be of some comfort to readers operating in the financial services sector to learn that, according to those interviewed for this paper, the sector’s work with the authorities through the JMLIT and other forums is perceived as an optimal example of public–private security cooperation and coordination. Indeed, one government official referred to ‘pretty good relationships’ in the sector, a view that was echoed elsewhere, with another stating that ‘the banking sector is exceedingly good at sharing within itself.’ During this research it became clear that the level and quality of public–private cooperation which exists in other sectors – both within CiSP and through other initiatives – varies considerably. Discussing the different approaches of sectors, one industry figure noted that ‘some are more mature than others’; the director of CERT-UK has similarly stated that more transportation and retail companies should be involved in CiSP.

Three Key Recommendations: Metrics, Coordination, Partnership

As far as information sharing on security issues is concerned, the financial sector appears to be operating at ‘well above average’, if not at the top of the class. However, it is also apparent that the JMLIT is faced with an immediate opportunity, as its future development is currently under active consideration as a result of its extension. While many more lessons could arguably be drawn from the analysis above, three particular recommendations arising from the experience of CiSP could be applied to the JMLIT, and could help to inform the next phase of its development.

Recommendation 1: Any public–private security partnership should establish measurable objectives that are co-designed and agreed among all relevant stakeholders from the outset. There should be tangible metrics that all parties agree to deliver, monitor and regularly review.

Doubts were expressed in the course of this research over the suitability of the metrics designed for assessing CiSP, and whether they are monitored effectively. While officials acknowledge privately that ‘metrics have always been a challenge’ for the partnership, it seems that ministers in particular may have been too eager to look upon the growing number of companies participating in the scheme as the main measure of its success. While this is arguably one useful indicator, it is suggested that more creative, nuanced measures of effectiveness are needed to assess the health of a public–private security partnership.

A key lesson from CiSP for the JMLIT, therefore, is that while implementing ‘at scale’ – that is, across the private sector – is important, the primary emphasis should be on achieving high-quality public–private cooperation rather than on the quantity of participants. During the course of this work, ideas offered on how to improve CiSP in this respect included: measuring the proportion of GDP that participants represent (rather than organisation numbers); measuring

34. Author interview with government official, by telephone, 4 March 2016.
35. Author interview with industry executive, by telephone, 10 March 2016.
38. Author interview with government officials, by telephone, 16 March 2016.
on an ongoing basis how many members actively contribute to the scheme;\textsuperscript{40} and, separately, measuring the amount of ‘actionable intelligence’ that has passed through the platform.\textsuperscript{41}

Another related lesson is that, whatever the agreed metrics, the objectives and measurement of such partnerships should ideally be agreed both in advance and on an ongoing basis, through an appropriate governance structure including representatives of both government and industry. While early agreement on the importance of CiSP was achieved through the Valentine’s Day ‘tea party’ in 2011, it is not clear how public–private engagement on cyber security issues should be configured on a continued basis at the strategic level. As a result, confidence in the scheme is apparently beginning to be eroded as the levels of genuine cooperation across the platform are called into question.

By contrast, the JMLIT seems to be on a much firmer footing, having arisen directly from the more obviously collaborative strategic forum, the FSF. However, there is no room for complacency. If the plan is to roll out a chosen partnership across a larger constituent base across the private sector – as has been the case with CiSP, and as is clearly the emerging plan for the JMLIT – there are also benefits to be had in ensuring that such deliberations are fully inclusive. In the view of the author, a period of consultation with maximum engagement on how the JMLIT should be delivered would help to ensure maximum stakeholder buy-in around the benefits and, indeed, expectations of participation in the future.

**Recommendation 2: To avoid duplication and confusion, proper consideration should be given at the outset to how any proposed public–private security initiative will connect to (if at all), and coordinate with, other existing methods of security cooperation.**

A key lesson from this research is that the UK’s security sector has lately experienced a considerable proliferation of public–private partnership initiatives, leading to a suspicion (if not some disgruntlement) within the sector that a lack of coordination may be duplicating efforts. The UK government’s proposal to consolidate the ‘alphabet soup’ of agencies and initiatives through the new National Cyber Security Centre (NCSC), to be launched in October 2016, represents a major attempt to address this outstanding problem in the cyber security sector, and one that is certainly extremely welcome.

That said, all concerned parties would also be well advised to manage their expectations around the extent to which any single structure may be able to achieve a perfect solution. This paper and many others are written in the knowledge that many different government departments and agencies are necessarily involved in the UK’s cyber security effort, and that more thorough consideration should be given to how coordination will be achieved between them at the design stage of such partnerships. Wherever ownership of such schemes may be located, it is vital that operational coordination is achieved among all relevant stakeholders, and across all pre-existing initiatives.

\textsuperscript{40} Author interview with industry executive, by telephone, 10 March 2016.  
\textsuperscript{41} Author interview with industry executive, by telephone, 18 March 2016.
The analysis above suggests that the chances of fully overcoming the many constraints associated with information sharing are not helped by an apparent lack of coordination across policy priorities and sub-sectors within the UK’s national security sector. Indeed, it would appear that, notwithstanding valuable initiatives such as CiSP, the structures being developed to encourage industry engagement in cyber security are not yet sufficiently mature to enable further strategic discussion of this crucial priority. Rectifying this is unlikely to be easy but, based on the experience of CiSP, early consideration of how an initiative connects to other existing efforts will be crucial for any public–private partnership. Related to this, and perhaps no less important, is the need to allow the flexibility for smaller groups of familiar companies, if not sectors, to cooperate with each other, even within the same overarching partnership structure. While a key aim must be to achieve effective coordination, therefore, the experience of CiSP suggests that there should also be room for a degree of information sharing between selected companies and sectors within any overarching framework—what might be called ‘minilateralism’ in public–private security cooperation.42

This emphasis on the importance of coordination, and of being able to coordinate flexibly, is particularly relevant for those charged with strengthening the JMLIT during its next phase of development. As the new NCSC is launched in October, for example, how (if at all) do those charged with its leadership propose to connect to such an important, emerging new initiative with others in the same sector? This is judged to be a crucial consideration as organisations involved in the JMLIT, such as the City of London Police, inevitably seek to engage with this new, well-funded structure.

**Recommendation 3: When designing security-related partnership initiatives, public and private sector stakeholders should devote more time to joint consideration of what each party seeks to gain from the ‘partnership’ in a practical sense.**

A degree of frustration exists among some of those knowledgeable about CiSP that the public and private sectors have different understandings of what ‘partnership’ means in relation to cyber security generally, and information sharing in particular. Descriptions of the relationship as resembling that between a parent and a child suggest that this is arguably the most challenging issue arising from the experience of CiSP to date, raising an important question: have the public and private sectors been clear enough with each other about how they understand ‘partnership’?

In the view of this author, the public and private sectors tend too frequently to ‘talk past each other’ when seeking to implement security partnerships such as CiSP and the JMLIT. On the one hand, senior government figures routinely stress the importance of partnership; yet, on the other, they seem also to want to place a high priority on encouraging the private sector to do more to protect itself. For their part, many private sector entities have arguably not been open enough about their capacities or their underlying commercial motivations, and seem reluctant openly to consider the effectiveness of their own contributions to CiSP. It is to be hoped, though this has not yet been tested, that this inclination arises from an honest desire to contribute to UK national security in a quiet way.

---

42. The author is indebted to Benoît Gomis for suggesting this idea.
It is against this backdrop that a key lesson emerges: that a ‘genuine’ or ‘active’ public–private security partnership will only be achieved if it is underpinned by mutual trust and honesty relating to how (and, indeed, whether) certain interests may ever be aligned. While this is perhaps obvious, and not to mention something of a common theme, it is a point that was stressed repeatedly by government and industry interviewees during this research. This is a highly topical and immediate potential learning opportunity for the JMLIT. As the government seeks ‘to include more banks and other financial services firms’ in the next phase of the initiative, for example, it is important to consider whether all parties associated with the scheme – both within the government and in industry – have been clear enough with themselves, and each other, about the potential resource implications of this ambition, and how they will work together to address them. In any event, other questions for consideration include: how many banks should be included? Which should be included? And who will measure this?

It is unfortunate that the necessary structures do not yet appear to be in place – certainly, not on a cross-sector basis – to address such challenging and potentially thorny questions. In a practical sense, as this Occasional Paper has shown, considerable effort has been made to address problems such as financial crime and cyber attacks at the operational level, but the UK arguably still lacks the strategic mechanisms that would help to facilitate this type of cooperation. How, for example, does the National Security Council and its associated architecture routinely engage with the private sector on organised crime and cyber security matters? There is currently no clear answer to this question, and the sense is that, at the highest levels of policymaking, public–private cooperation is often seen as a secondary, ad hoc activity, an optional extra to be addressed on a sector-specific basis.

In summary, the question of how the government might better engage industry on security issues, and vice versa, has not yet been sufficiently debated. As one interviewee powerfully argued, a key lesson is that all those concerned with developing public–private cooperation should be ‘making sure industries are brought along in [the] development of [an] idea’. It should be noted that, institutionally, the structures that currently exist in the UK have a very mixed record of enabling this type of discussion.

---

43. In discussing cyber security partnerships in the US, Germano also notes the importance of trust and ‘ongoing dialogue among stakeholders regarding expectations’. Germano, ‘Cyber Security Partnerships’, p. 10.
44. Author interview with government officials, by telephone, 16 March 2016; author interview with industry executive, Surrey, 24 February 2016; author interview with industry executive, by telephone, 11 March 2016.
47. Germano has made similar calls to ‘institutionalise the processes by which the public and private sectors can cooperate to address the cyberthreat’ in the US context. Germano, ‘Cyber Security Partnerships’, p. 11.
IV. Conclusion

Everybody is recognising that partnerships are the way forward.¹
Chris Gibson, director, CERT-UK, September 2014.

This occasional paper has offered lessons for the JMLIT from an analysis of the origins, characteristics and effectiveness of public–private cooperation in the UK’s cyber security sector, specifically the experience of CiSP. While noting that significant effort has been directed towards the development of stronger public–private cooperation around the sharing of cyber threat information through CiSP, and the initiative has undoubtedly added value, this paper has highlighted a number of limitations and also lessons learnt from the experience which could be usefully applied to the JMLIT.

How can this happen in practice? The UK government and its partners are presented with an immediate opportunity because many authorities appear to be coming to the conclusion that public–private security cooperation (including, but not limited to, information sharing) is an essential component of the response, and that new thinking will be needed on this issue. Furthermore, initiatives such as the JMLIT and the proposed NCSC are currently at an early, formative stage of development, thus offering the potential for the principles of a genuine partnership to be ‘designed in’ from the outset. It is advised in this context that the JMLIT takes account of the three key recommendations offered in this paper – the need to establish appropriate metrics, to drive through more effective coordination, and to develop better understanding of ‘partnership’ – as it moves towards its next phase.

Whether public and private sector partners involved in initiatives like CiSP and the JMLIT are fully committed to engaging in more open, honest dialogue and stronger cooperation in addressing security challenges is yet to be seen; there is some evidence to suggest that, so far, in some areas, ‘neither side sees it as a partnership’ in the proper sense of the word.² In the meantime, it would appear that, however ‘dysfunctional’³ the partnership can sometimes be, few would now doubt that, when addressing transnational risks such as financial crime and cyber insecurity, public–private cooperation is an essential component of the policy response.

¹ Gibson, ‘Partnership with Industry’.
² Author interview with industry executive, London, 19 February 2016.
Dr Hugo Rosemont is Policy Adviser on Crime, Security, Risk and Safety issues at the British Retail Consortium (BRC). Prior to his current appointment, he served as Teaching Fellow and Assistant Director of the Centre for Defence Studies within the Department of War Studies at King’s College London. In April 2015, he was awarded his PhD (also with King’s College London) with a thesis on the ‘security-industrial complex’ that reassessed the origins, characteristics and consequences of the private sector’s involvement in the counterterrorism aspects of contemporary UK national security strategy. Previously, Hugo served as Policy Adviser (Security and Resilience) to ADS – the organisation advancing the UK aerospace, defence and security industries. In this role, he provided security policy advice to the ADS Security Sector Board and the UK Security and Resilience Industry Suppliers Community (RISC). He was also a member of the Home Office’s Olympic and Paralympic Industry Advisory Group and served as Security Executive to both the winning London 2012 Olympic bid team and the London Organising Committee of the Olympic and Paralympic Games (LOCOG). In addition to his current role at the BRC, Hugo lectures and consults in an independent capacity on public–private security cooperation. His commentary has appeared in media outlets including, among others, the BBC, ITV, France 24, The Financial Times, The Independent, The Sun and The Guardian. He has been interviewed by John Humphrys on the BBC Radio 4 Today programme, and by Nick Ferrari on LBC. He writes this paper in an independent capacity.