THE WINSTON CHURCHILL MEMORIAL TRUST OF AUSTRALIA

Report by – David Connery – 2015 Churchill Fellow

THE DONALD MACKAY CHURCHILL FELLOWSHIP TO ENHANCE INFORMATION SHARING BETWEEN LAW ENFORCEMENT, BUSINESS AND COMMUNITY ABOUT ORGANISED CRIME - USA, CANADA, UK, FRANCE, NETHERLANDS, ISRAEL

I understand that the Churchill Trust may public this report, either in hard copy or on the internet or both, and consent to such publication.

I indemnify the Churchill Trust against any loss, costs or damages it may suffer arising out of any claim or proceedings made against the Trust in respect of or arising out of the publication of any report submitted to the Trust and which the Trust places on a website for access over the internet.

I also warrant that my final report is original and does not infringe the copyright of any person, or contain anything which is, or the incorporation of which into the final report is, actionable for defamation, a breach of any privacy law or obligation, a breach of confidence, contempt of court, passing-off or contravention of any other private right or of any law.

Signed: David Connery Dated: 8 June 2016

Table of Contents

Executive Summary 5

The study 6

The problem 6

Aim and method 7

Report structure 7

1. The subjects 8

Transnational, Serious and Organised crime 8

The 'triangle of shared interests' 9

2. The object 12

Defining information sharing 12

Types of information shared 13

Types of sharing arrangements 14

Potential benefits and down-sides 14

What information does government, business and the community want to share about organised crime? 17

What kind of information does government want to receive and share? 17

What kind of information does business want to receive and share? 17

What kinds of information does the community want to receive and share? 18

On balance, it's worth sharing information about crime 20

3. The mechanisms 21

The dimensions of sharing 21

Informal mechanisms 21

Formal mechanisms 22

4. Factors influencing inter-sectoral information sharing about crime 27

Factors enabling information sharing 27

Factors inhibiting information sharing 30

Conclusion 33

Annexes 34

References 34

Abbreviations 38

Annex A: Israel 40

Context 40

Sharing information about financial crime 41

Counter-terrorism 42

Cyber security 42

Business perspectives about information sharing 43

It's all in the network 43

Factors that promote information sharing about organised crime in Israel 44

Factors that inhibit information sharing about organised crime in Israel 44

Annex B: United Kingdom 45

Context 45
Countering fraud, UK Style 45
The anti-fraud landscape in the UK 46
The legislative framework 46
Sharing information about fraud—the UK practice 48
Information sharing to counter crime against business and the community 50
Implementing local counter-crime strategies 50
Programs to counter crimes against business 52
Forward leaning and risk accepting 53
Factors that promote information sharing about organised crime in the UK 54
Factors that inhibit information sharing about organised crime in the UK 54
Annex C: The Netherlands 55
Context 55
Dealing with organised crime – Amsterdam style 57
The CT-Infobox 59
A new model of collaboration: ECTF 61
Multi-national and public-private: EC3 62
Might the situation change? 63
Factors that promote information sharing about organised crime in the Netherlands 64
Factors that inhibit information sharing about organised crime in the Netherlands 64
Annex D: The United States 65
Context 65
The FBI and information sharing 67
Information Sharing and Analysis Centres (ISACs) 70
National Cyber-Forensics and Training Alliance 73
New York Police Department 74
New York City Emergency Management (NYCEM) 77
Social media and web-based platforms 77
Bulk data 78
Strong, contrasting pressures on information sharing 79
Annex E: Meetings 81
Israel 81
United Kingdom 82
Netherlands 82
United States 83

About the author

Dr David Connery is Head of the Strategic Policing and Law Enforcement Program at the Australian Strategic Policy Institute. His previous career experience includes service in the Australian Army and the Department of the Prime Minister and Cabinet, and secondments the National Security College and Office of National Assessments.

Contact: davidconnery@aspi.org.au

Acknowledgements

Special thanks go to the Churchill Trust; the Rotary Clubs of Griffith NSW; Peter Jennings, the Executive Director at ASPI; and my always inspirational family.

This report is dedicated to the eighty people interviewed for this project, for they work tirelessly to fight organised crime in their respective countries. It's hard to imagine what the world would be like if good people like them, and their thousands of colleagues, were not willing to do so.

Executive Summary

This report examines how government, business and the community in four nations share information about organised crime. The report begins by defining information sharing as 'the trusted exchange of relevant knowledge or data between organisations to enhance their mutual objectives'. The types of information shared are then divided into two: case information that involves data about individuals who are usually suspected of involvement in criminal activity; and bulk data that includes people in a given set regardless of any possible connection with crime.

The fieldwork involved eighty interviews, including visits to or discussions about a range of information sharing mechanisms in the four selected nations. These mechanisms were broadly differentiated by their location (within or outside government) and the nature of the sharing interaction (exchange or collaboration). The vast variety of mechanisms used in the four nations shows that information sharing is valued and strongly shaped by the particular national context. This means some countries rely heavily on informal systems, others have large numbers of specialised exchanges, and some are more risk accepting in their arrangements than others. The fieldwork showed that a wide range of options for sharing information about crime exist, and that Australian authorities and businesses might wish to consider a number of these in more detail.

This research found both upsides and downsides to information sharing about crime. Some benefits are clear, including the opportunity to shape better interventions and build economy of effort in activities. While these upsides are undoubtedly attractive, it seems that the possible downsides of sharing—such as loss of control, potential to compromise of sensitive activities, or an unwillingness to risk breaking the law—were viewed as considerably strong downsides to sharing. Still, it is clear that sharing must occur. That's because the scale of the challenge posed by organised crime—and the speed, reach and depth of penetration that the internet enables—means information sharing is critical for all three groups.

This report explains that information sharing is best promoted by building a strong sense of shared interest among the participants, and then developing a strong system for information sharing that is governed by understood rules. This finding stands in contrast to those who emphasise interpersonal trust as the basis for sharing. Factors that work against information sharing about crime include legislative barriers and complexity, poor value propositions around sharing, the self-conceptions of the actors and what they value information for, and cultural barriers. Such barriers include a culture of secrecy in government, the lack of willingness to expose possible flaws, and the view that 'information is power'. These are perhaps the most powerful inhibitors to sharing. Any effort to enhance Australia's methods of sharing information about organised crime should be designed to cope with these inhibitors while making best use of the factors that promote this vital activity.

For the right reasons, in the right ways

A four-nation survey of information sharing about organised crime between law enforcement, business and the community

by Dr David Connery

"All that is necessary for the triumph of evil is for good men to do nothing."
The memorial tribute to Donald Mackay, 1933-1977

The study

The problem

Information is an important commodity that, if released carelessly, cannot be controlled. This property makes information sharing a very sensitive topic because done in the wrong way, so that it falls into criminal hands or maligns lawful individuals, the act of sharing could have serious repercussions for justice, law enforcement and the community at large. Such a situation is in nobody's interest.

Information is the life-blood of modern law enforcement, but the information needed by law enforcement is not held in a single repository. Far from it. Information holdings are highly diffuse, and important evidence can be held not only by other government departments, but also the business and public. Holdings can also be insecure, providing a tempting target for hackers and thieves. So bringing the right information together in the right way, form, and time is an immense shared challenge for all concerned in this activity.

Finding suitable ways to share information about organised crime is therefore a critical task for Australia's government, business sector and community at large. This is particularly so as major debates rage about the balance between security and civil liberties; the retention and use of data and privacy; the valid role of encryption, and the increasing austerity being imposed on government and businesses directly, and the public at large indirectly. Identifying ways to effectively and fairly share timely information and bulk data is a task that is becoming more challenging every day. New ideas are needed.

Aim and method

This project examines three information sharing relationships—among government agencies (especially law enforcement), the business sector, and the community—in four different nations.

The aim of this report is to identify the basic frameworks used to share information about crime, especially but not only organised crime. This framework will necessarily include definitions of the subjects of the study (the actors involved) and the object, enhanced information sharing. The resulting framework will be illustrated with examples from the four countries visited during the fieldwork phase, which were Israel, the United Kingdom, the Netherlands and the United States. The study will also identify general factors that promote and inhibit information sharing about crime.

Fieldwork for this report was made possible by a fellowship from the Winston Churchill Memorial Trust. More specifically, this fellowship is supported by the Rotary Clubs of Griffith, NSW, who maintain the Donald Mackay Fellowship for research into countering organised crime. The assistance of Peter Jennings, Executive Director of the Australian Strategic Policy Institute and my employer, is also appreciated.

Research for this report is based on a review of the relevant literature and interviews with over 85 experts from the government, community and business sectors from the four nations visited. These countries were chosen for the study because they are all liberal constitutional democracies, have significant safeguards in place to protect privacy, and conduct information sharing about crime. These criteria mean the types of mechanisms used (or not) are likely to be relevant to Australia. Semi-structured interviews were used with each of the experts, nearly all lasted 90-120 minutes, and many were amplified in follow-up correspondence. The results of the study include assessments of the factors promoting or inhibiting information sharing in each country, a description of the mechanisms used, and a model that allow information sharing mechanisms to be categorised.

Report structure

This report is structured into four substantive sections. The first defines the subjects of the study—organised crime, and the government-business-community 'triangle' that needs to cooperate against these nefarious actors. The second section describes the object of cooperation, information sharing. This section starts by defining information sharing, and then moves to an examination of the reasons, types, risks and rationale for doing so. Section 3 develops a model for information sharing that is based on examples observed during the four-nation study tour. Section 4 draws conclusions for the study in the form of general factors that inhibit or promote information sharing about organised crime.

Also included, as annexes to this report, are short papers describing the context for information sharing about organised crime in each of the nations visited, and explanations of the information sharing mechanisms discussed during the visits. A list of interviews by country is also included.

1. The subjects

This research report is essentially about the relationships between and among two different subject groups. On one side sits organised crime: a broad grouping of nefarious actors who use criminal methods to exploit illicit and legitimate markets for private gain. The relationships among organised crime actors are not a topic for discussion here, but relationships among the second group are. This group is the government, the business sector and the community: a 'triangle' of actors who share—at least to some degree—a shared interest in combating organised crime. This section describes each actor group at their most general level as way to frame the later discussion of information sharing.

Transnational, Serious and Organised crime

Defining transnational, serious and organised crime succinctly and comprehensively is difficult. As my colleagues identified in a recent special report for the Australian Strategic Policy Institute, there are many definitions—around 180, by one count.[1] Some require the presence of an ongoing criminal activity that uses methods such as money laundering, identity crime, violence, corruption and extortion to achieve the criminals' goals. Others are broader, focusing more on the seriousness of the crime or their capacity to operate across jurisdictions. Organised crime (as this activity and actor group will be called throughout) operates in illicit markets, legitimate markets, and in any 'grey areas' that might exist: indeed, anywhere where criminal attitudes and methods can be used to their personal advantage. What's more, organised crime has evolved over the last few decades in ways that move beyond the hierarchical 'mafia' organisational styles that featured among the first definitions of organised crime. These 'old style' gangs have now been joined by more amorphous and fluid networks of actors that provide services or share tasks among each other to their mutual criminal benefit.

This report uses Australian legal definitions, which means that serious and organised crime:

- Involves two or more offenders and substantial planning and organisation
- Usually involves sophisticated methods and technologies (but not always)

[1] D. Connery, C. Murphy and H. Channer, 'Web of Harms: Serious and Organised Crime and its impact on Australia's interests,' Australian Strategic Policy Institute Special Report 81, Canberra, 2015. The following section borrows heavily from pp. 3-4.

- Involves serious offences that are likely to attract a sentence of three years or more, such as theft, illegal narcotics dealings, extortion, violence, bribery or money laundering—often in conjunction with offences of a like kind.

The characteristics of organised crime groups vary within and among the countries studied for this report. There is no single or predominant type of group structure; older traditional 'mafia' style hierarchies might still prevail in some countries, but looser 'networks' involving cooperation between often disparate and transnational groups operating on different parts of the criminal enterprise are common too. The motivation for serious and organised criminals is generally personal profit and self-preservation, although criminals can be interested in power, honour and gratification too. In addition, the following characteristics usually apply:

- Organised crime generally works in illicit markets but it exploits legitimate markets too.
- There's an important financial dimension, particularly in efforts to launder money, hide criminal wealth through complex structures, attack victims' financial assets or intermingle legitimate trade and business with criminal activities. These crimes are often supported by 'professional facilitators' with legal, accounting or financial expertise.
- Violence was once considered a defining characteristic of serious and organised crime methods. However, with the increasing prevalence of the cyber environment as a vector and target for organised criminal acts and major frauds that undermine economic strength that is not always so today.[2]

Serious and organised crime can be organised and perpetrated solely within one country (i.e. 'domestic') but it's very common for groups to have overseas, or 'transnational', links today. Transnational crime involves criminal groups that operate in more than one national jurisdiction, or crimes that are prepared in or have effects in more than one national jurisdiction. As a result of this transnational trend, it's becoming increasingly difficult to identify the location of the source, all possible harms and the responsible jurisdiction for serious and organised crime. So, while the transnational element needs to be highlighted and their crime is routinely serious, this report sticks with the term 'organised crime' for simplicity's sake.

The 'triangle of shared interests'

The government, business and community sectors are considered in this paper as a triangle linked by their shared interest in combating organised crime. This is

[2] Australian Crime Commission (ACC), *Organised Crime in Australia 2015*.

a heroic assumption. There are differences in attitudes, commitment and resources within these groups, so each contains subsets that warrant explanation. The groups will also change over time, as some elements of each group evolve or play different roles at different times, as the media does.

The first actor group of the triangle is the government, with law enforcement agencies being a key subset. These agencies are given, by law or accepted practice, a role in the criminal justice system that might include research, criminal intelligence, investigation, public safety, prosecution, judgment and correction. A range of other agencies with roles including policy setting, national security information protection, foreign affairs, and regulation will also play roles in the justice system. Of these peripheral justice actors, regulators are especially important because they may have the ability to set rules, conduct investigations and take briefs of evidence to the police or prosecution services. The government might also form subgroups that create links with the other actors. These might include public-private partnerships, task forces that operate within public agencies, and international partners. Social service, economic and defence agencies are also likely to be relevant to fighting organised crime, even though their primary responsibilities lay in other areas.

The second actor group is business, which are profit-making entities that deliver goods or services within a market. Major business entities are usually incorporated by law and many are regulated by government agencies. This group can be subdivided into those who provide services similar or complementary to law enforcement (such as physical and cyber security firms, forensic analysis services); and the much larger grouping who rely on law enforcement and regulation to sustain suitable market conditions. Some overlap will exist between these groups—security firms are also regulated and rely on a market, some large trading companies have investigative units that help law enforcement, and financial firms play a key role in the anti-money laundering and counter-terrorism financing (AML/CTF) system—so the distinction within this grouping is not applied rigidly. Nor should the ability of business and law enforcement to 'cross over' be neglected. In the examples below, we'll discuss examples where business directly funds law enforcement agencies, and instances where business are 'co-providers' of security.

The third group is the community, with comprises the individuals in society ('the general public'); academics and think-tanks who conduct research and contest policy advice; and groups of individuals who come together to satisfy their mutual, non-economic interests (often called 'not-for-profit', 'civil society' or 'third sector' groups). Not-for-profit groups (NFP) will play different roles in society and, as we'll see, can be involved in two-way information sharing and partnerships with law enforcement under certain circumstances. NFP groups might also provide complimentary services to government and business, such as welfare and social housing services. In all circumstances, NFP, researchers and the general public are the recipients of police information in terms of warnings and crime-prevention advice, and are sources of information about specific crimes (often called 'tip-offs'). Some bring matters to public and government attention, and recommend or advocate for particular solutions to national problems.[3] When operating like this some community groups can act like the media, albeit on a different scale.

The place of the media in this triangle is ambiguous. Assuming it operates separate from the government (as it does in western democracies), the media can be a business with peculiar needs. It too needs protection and advice on crime prevention, but it also needs content: publishable information about organised crime. The media is also a reflection of the community – they report on issues that matter to the community, gather and represent community views, and provide an outlet for members of the community to express views. This ambiguity means the media is well-represented in the middle of the triangle of shared interests.

Linking these groups is clearly challenging, for another filter must be used: their desire, willingness and capacity to counter organised crime. We cannot assume that every element within the triangle of shared interests actually shares the common goal described here. For instance, professionals like some lawyers, accountants and real estate agents actively facilitate organised crime by helping criminals to enter into or through the legitimate economy. Some members of the public are supportive or tolerant of organised crime. Some members of the government might be corrupted by crime. The role played by these elements will be neglected in this report, so we can focus on the key issue.

That key issue is straight-forward: countering organised crime is not the sole responsibility of any one group over another. Each has a part to play. Further, they can best perform their roles and achieve their individual and shared objectives if each hardens themselves against organised crime by reducing vulnerabilities and by sharing information with each other.

Still, that doesn't mean information sharing is easy or that its many complications have been overcome. Indeed, the 2015 version of Australia's National Organised Crime Response Plan highlights the weaknesses in information sharing between government, business and the community.[4] Before we examine the different models for how information sharing is done in overseas jurisdictions, it is worth defining the topic and establishing its utility. After all, we should not assume that information sharing about organised crime is unambiguously good.

[3] For instance, the role of Israeli NFP groups in analysing and highlighting human trafficking in that country was mentioned in an interview as an example.

[4] Attorney General's Department, *National Organised Crime Response Plan 2015-18*, pp. 19-20 describes the community as 'underutilised', and that it is harder to gain traction to combat organised crime in industries whose profits are only marginally affected by organised crime. There is also a general desire to reduce the cost of maintaining relevant government-business relationships. There is also a strong focus on enhancing information sharing within and between governments: while related, this challenge lies outside the scope of this paper.

2. The object

Defining information sharing

Information sharing is the object of the relationships within the triangle of shared interests. While a seemingly straight forward concept, information sharing can be viewed in very different ways. A mechanistic view sees it as a function of taking inputs and creating outputs:

> Information sharing in criminal justice involves collecting and organisation facts and figures (i.e. data), giving context to data, and providing information to various other individuals and/or organisations for strategic and operational decision making.[5]
>
> Information sharing involves the transfer of information from one agency to another.[6]

Others see information sharing as a social activity:

> Information sharing can be a volunteer behavior to provide information to other people who have information needs.[7]

Or they define it in a way suited to their specific sector. In an example pertaining to technology industries, the authors define information sharing as:

> …the exchange of a variety of network and information security related information such as risks, vulnerabilities, threats and internal security issues as well as good practice.[8]

In this report, information sharing will be defined in socio-mechanical terms as the trusted exchange of relevant knowledge or data between organisations to enhance their mutual objectives.

While a start, the definition does not capture the distinctions between the types of information that can be shared, or different types of sharing mechanisms that can be used. These are important because the nature of the information sharing activity will often be enabled or constrained by additional factors such as law, needs and working culture.

[5] D. Plecas, A. McCormaick, J. Levine, P. Neal and I. Coen, 'Evidence-based solution to information sharing between law enforcement agencies', *Policing: An international Journal of Police Strategies and Management*, Vol. 31, No. 1, 2011, p. 121. See also Department of Homeland Security, 'Local Anti-Terrorism Information and Intelligence Sharing: Overview', n.d., p. 1, available: https://www.hsdl.org/?view&did=765456.

[6] UK Home Office, 'National Support Framework: Information Sharing for Community Safety', HM Government, 2010, p. 5.

[7] T.M. Yang and T.A. Maxwell, 'Information Sharing in Public Organisations: A literature review of interpersonal, intra-organisational and inter-organisational success factors', *Government Information Quarterly* 28, 2011, p. 165.

[8] Neil Robinson and Emma Disley, 'Incentives and Challenges for Information Sharing in the Context of Network and Information Security', European Network and Information Security Agency, 2010, p. 9.

Types of information shared

It is important to distinguish between the types of information about organised crime that can be shared, because one type tends to be less problematic in law than the other. Leaving aside the informal 'tips' that pass between individuals, formal systems will often see two broad types of information: 'case information' and 'bulk data'.

Case information is characterised by the direct exchange of data (and sometimes intelligence, which can be defined as data analysed to provide judgments for decision-makers) based on a specific request. The information provided will often include names, personal details, location, assets, transaction records, and the like. Case information is usually provided after a direct request is made about a particular individual, or it may be presented as an intelligence or investigation 'package' by businesses to stimulate law enforcement or other responses.

'Bulk data' refers to structured or unstructured data sets concerning a relevant activity.[9] Bulk data might be used for research and intelligence purposes to examine the activities of many people at the same time, perhaps with the view of isolating criminal activity and identifying an individual perpetrator. It will include references to more than one individual—often thousands at a time—and unless it is 'scrubbed', bulk data will often contain personally-identifiable information (PII). As a result, bulk data tends to contain information about a number of people who are not involved in crime, as well as people who are.

Both types of information can be shared, but case information (when exchanged between authorised groups) tends to be less problematic. That's because it's usually highly specific, and standards such as 'suspicion' of involvement in a crime can be applied more readily to judge whether release is appropriate. This survey found numerous instances across all four national jurisdictions where such information is routinely, safely and expeditiously shared.

Bulk data can be shared too, and it often is. For instance, de-identified crime statistics can often be provided to researchers and the public with little controversy. Publicly-available bulk data (the extent of which varies from jurisdiction-to-jurisdiction) is also less of a concern. However, bulk data that can be used to identify individuals, especially those not suspected of crimes, tends to be highly concerning and broadly illegal in the jurisdictions surveyed for this report. Pejoratively known for facilitating 'fishing expeditions', this type of data sharing can come afoul of informed consent and proportionality provisions in some legislation.

[9] In general terms, 'structured' data has a high degree of organisation, and may be contained in databases that are searchable by simple, straightforward search operations. Unstructured data is essentially the opposite, and includes formats like video and images (see http://www.brightplanet.com/2012/06/structured-vs-unstructured-data/).

Types of sharing arrangements

The report will also distinguish between ‘information transfer’ and ‘information collaboration’ as types of information sharing arrangements.

Societies are always engaged in the information transfer business: this involves the straight passage of useful information from one party to another. For example, the general public will nearly always provide ‘tips’ to the police; not-for-profit organisations may examine crime areas and provide reports; and business will provide information as required by law, such as suspicious matter reports. For their part, police will provide warnings to the community and business about threats and advice to prevent crime. There are very limited interactions between the sources though, and when interaction occurs it tends to be in the form of sequential responses to each other.

Information collaboration is different. This activity usually occurs within formal, structured systems, where the partners work together to solve shared problems through the exchange of information. Sharing is interactive, trusted, based on agreed rules and often in real-time. This report will highlight a number of collaborations, and identify factors that allow these bodies to function within the law, the defined purpose, and operate sustainably in ways that satisfy partners, oversight mechanisms and the general public.

We should not infer that one type of arrangement is superior to another from this categorisation. As with most things, it’s more important to have the most appropriate arrangement to share than to have the one that sounds the most modern. This means choosing the best form requires a keen understanding of why information sharing is needed in the first place, and the up-side and down-side risks associated with the options for sharing.

Potential benefits and down-sides

The hypothesis under examination in this project holds that information sharing about organised crime has benefits for the national interest, economy and community as a whole. Cooperation between government, business and the community is required to meet these benefits, which include:

- **Understanding the problem.** Shared information can help identify the scope and scale of a problem, relationships between actors involved in that problem, and the pattern of the actors’ interactions in time and space. Since information sharing also increases the number of people engaged in problem solving and so introduces additional diversity into analysis, there is a chance to enhance assessments by integrating or testing different perspectives.[10]

[10] Nathan A. Sales, ‘Mending Walls: Information Sharing after the PATRIOT Act’, *Texas Law Review* 88: 2009-10, pp. 1801-2.

- **Best use the powers available.** Information sharing can promote cooperation among legitimate actors, including by promoting an understanding of the powers and capabilities of each. This can reduce overlap and increase the incentives to cooperate.
- **Better interventions.** Understanding the respective strengths, weaknesses, motives and methods of the actors involved (especially those causing threats to community) helps legitimate actors identify ways to protect themselves, prevent access by illegitimate actors, respond to threats, and recover from attacks. Information sharing promotes cooperation as shared objectives are established and a common awareness of the situation is developed. Information from government, business and community sources is also a key input to intelligence led policing models.[11]
- **Economy of effort.** An adage in the information sharing business goes, 'collect once, share many times'. Information sharing can (should) reduce the amount of effort expended to collect data, reduce the frequency of information requests from businesses and the public, and increase the utility of each individual data set. Agencies can also be more specialised in their data collection, and so reduce duplication of efforts and encourage compliance with law. In some ways, information sharing can make government less intrusive because fewer agencies need to collect the same data.[12]

Still, information sharing can have down-sides. These negative consequences are often privileged in professional interactions that might warrant information sharing—leading to limited or no sharing between the parties at the extreme. The key downsides include:

- **Compromise of methods and sources.** Releasing information can sometimes reveal to others the method used to obtain the information, or the source of the information.
- **Compromise of operational activities.** The inappropriate release of information about operational activities, like investigations, can lead to the compromise of evidence and make the activities unsafe for participants.
- **Breaches of rights, laws and freedoms.** The release of information has the potential to breach rights such as privacy or data protection laws in many countries. In other cases, sharing information about citizens raises the prospects of a 'surveillance state' whereby information given by customers to business is used by government agencies to unnecessarily track law-abiding people. The existence laws incompatible with western

[11] J.G. Carter, 'Inter-organizational relationships and law enforcement information sharing post 11 September 2001', *Journal of Crime and Justice*, 38:4, 2015, pp. 523-4.
[12] Sales 2009-10, p. 1798-99.

human rights standards and authoritarian governments in some countries complicates this risk when information gained domestically is shared with other countries.

- **Loss of context.** Data released can sometimes be stripped of its context. Aside from the mistakes non-experts might make in assessing specialised data, other problems with interpretation can occur once data has left the originating agency. For example, people might be admitted to a mental health program for a number of reasons and for conditions of varying severity. Therefore assuming that a person has a serious mental health issue based on admission data is not necessarily accurate.
- **Conferring unequal advantage.** Information sharing with selected partners has the ability to confer an advantage to one party that similar parties will not get. This might include insights into market conditions or competitor vulnerabilities. This risk is most relevant in small information sharing forums where smaller companies or average citizens do not have the resources to participate.
- **Reducing relative advantage.** If information is power, releasing information can reduce the relative advantage of one party over another, or complicate the working life of those who must now answer more questions about their activities because 'outsiders' now know about those activities.
- **Imbalance between effort and reward.** Information sharing is not a 'cost free' activity. New data sets may be required, data may need to be 'scrubbed' of PII or presented in different formats, people will need to assemble and reply to requests, and people may be requested to participate in task forces or working groups. All of these activities cost money, and it may be that little is returned for that effort. Situations like this can lead managers to see information sharing as unwarranted and uneconomic for them.
- **Self-incrimination.** Sharing information might provide others with evidence of wrong-doing, poor practices or vulnerabilities.
- **Missed opportunities.** The decision not to share might mean opportunities to address problems, create new value or save money might be missed.
- **Unmet responsibilities.** The failure to share information can also result in severe criticisms of organisations, as the US Intelligence Community found after the 9/11 terrorists attacks, or in cases where real harm that befalls vulnerable people may have been avoided if agencies shared information.

While the down-sides listed are more numerous that the identified benefits, that should not discourage well-planned efforts to share information. Fortunately, there are a number of different models that can be used to ensure information sharing is healthy and cost-effective, and these are described in section 3. Also, different kinds of information can be shared. This distinction is important because sharing some data to counter organised crime is usually considered legitimate, while sharing other types of data raises privacy and other concerns.

What information does government, business and the community want to share about organised crime?

The remarks above addressed to the potential hazards contained within the act of sharing information about serious and organised crime. What needs to be addressed next is the type of information that can or should be shared. This is important to outline because the needs and wants of each group can not only differ, but be in stark contrast with each other.

What kind of information does government want to receive and share?

In general terms, government needs can be divided into two levels. On a broad level, government wants to show action against visible crime, and this may include meeting election or policy commitments. Government will also want to advertise its achievements, be that through improved crime statistics or successful operations and initiatives. Satisfying this type of information need usually involves statistical data or reports of major police activities. Detailed evaluations might also help explain and advertise successful programs.

Law enforcement's main needs revolve around 'actionable' information. This might be information that adds to an intelligence picture, but information that helps investigations is most prized. This preference reflects the primary self-conception of most law enforcement agencies (especially police agencies) as being responsible for bringing criminals to account through the courts.

Law enforcement also needs information from business and the community about the ways to fight crime. In particular, many large business have considerable experience in fighting crime in their industry sector (including overseas sources of information), while others have specialist intelligence, forensic or technical skills. Sharing this kind of information can help law enforcement to warn, prosecute or protect; and commercial relationships may be established to provide this kind of information sharing.

What kind of information does business want to receive and share?

Businesses desires for information differ in many respects, but they are linked around a tight focus on competitiveness and business survival. This means businesses want information tailored to their need for protection from crime, especially their immediate needs. They express a very uneven desire to receive broad, generalised information, but most appreciate and prefer tailored advice and threat alerts. There seems to be some interest—but not much—in forward-looking advice about emerging threats, new technologies and vulnerabilities, and ways to protect themselves from the attendant criminal threats.

Businesses also desire very specific information about criminal threats and methods, right down to the identity of customers who are criminal threats to them. This type of information might include account details, advice of fraudulent claims made against other business, or images of criminals.[13] Others, especially internet service providers and larger corporations, want details of cyber threats such as IP addresses and identities so they can take action to block malicious activity. This information represents their 'actionable intelligence'. However, it's possible that businesses want information that's further up the chain of discovery, but don't know how to ask. That information would be generated as new threats are identified, and involves businesses and law enforcement working collaboratively in 'joint discovery' on both criminal methodologies and perpetrators.[14] Such collaboration can already be seen in some of the information sharing mechanisms describes in the next section.

A third type of desired information is about particular events and emergencies that may affect business operations or continuity. This type of information also needs to be made as specific as possible, largely because information that is difficult to use can create confusion and increase costs.

What links these information desires is relevance and immediacy: and this is where government and business tend to diverge. Governments—especially at the federal or national level—generally want to deal with information on a large scale, to the broadest number of people possible. That doesn't preclude very direct and intimate sharing arrangements, as the examples in the next section will show. But intimate sharing is costly for government and gets harder to achieve as the number of interested businesses increases. Scale is preferred as it is cheaper to deliver.

Timely information can also be hard to share. Sharing with business might be contrary to the interests of law enforcement agencies, especially when legislation prohibits sharing or where investigations or court proceedings are underway. By the same token, businesses do not want to share information that might incriminate themselves or expose wrongdoing. This reticence is particularly applicable when disclosure to those who regulate them, or might hold them accountable to the law, might expos eth firm to penalties or even criminal prospection. Disclosure might also expose the business to reputational damage, which for many presents a key risk and an inhibitor to sharing. That said, there are a number of ways that government and business are sharing information in intimate ways in all four nations visited, which gives room for optimism about the prospects for finding effective information sharing mechanisms in different circumstances.

What kinds of information does the community want to receive and share?

It is harder to pin-point what kind of information the community wants to receive and share. Certainly, accurate information for their needs is one, and this

[13] Carter 2015, p. 525.
[14] Discussion with Australian government official, 23 May 2016.

has been long-standing. What seems to be changing is the desire for more specific information that's tailored to the individual's needs. This may involve alerts and warnings, applicable to their 'microclimate' or neighborhood. It might also involve specific crime prevention advice.

The information that the community is willing to share is highly contextual. As the Pew Research Center found through a recent survey:

> …the phrase that best captures Americans' views on the choice between privacy vs. disclosure of personal information is, "It depends." People's views on the key tradeoff of the modern, digital economy – namely, that consumers offer information about themselves in exchange for something of value – are shaped by both the conditions of the deal and the circumstances of their lives.[15]

But willing or not, people are sharing more and more personal information, and detailed information about their activities. While this is not the place to explore the factors relating to individual information sharing decisions, three drivers of that sharing are clear.

Firstly, there has been a huge increase in the amount of information available to crime, law enforcement and business about individuals. That increase introduces challenges with storage, security and analysis. These in turn increase the cost of holding data and encourages those holders to monetize it. There is also a greater chance for others to analyse the data for different purposes, such as criminal investigations. Inconsistent security standards among holders also increases the risk that data will be stolen and misused.

Secondly, actors have different interests in that information—although these interests can be symbiotic at times. For instance, many companies collect masses of data about their customers, and they might on-sell that to other business for marketing purposes. That same data, especially data relating to a person's identity or credit card, also provides a lucrative trove for criminal groups. Police investigations routinely use information from companies, especially telecommunications metadata, transport bookings and the like. The different ways data can be shared, used and re-purposed means that the consumer really has little say in who gets access after they provide it.

And thirdly, businesses can help people, including criminals, by providing services like encryption or anonymous account holdings that disguises data. These services complicate information sharing and frustrate law enforcement, tax departments and regulators.

In all these cases, the public's role as a consumer will differ widely. Not-for-profit and researcher groups will have more specialised information need than the general community, and they are likely to be well-placed to use that information.

[15] Lee Raine and Maeve Duggan, 'Privacy and Information Sharing', Pew Research Center, 14 January 2016.

In some cases observed, not-for-profit groups will provide services to government (such as accommodation and welfare) that will put their holdings on a par with what a government might hold in other countries. Researchers have long demonstrated their value to law enforcement, especially as the need for data and analysis becomes more valued by agencies.[16] Individuals can also play important roles in various initiatives to counter organised crime, such as by reporting their observations through web-based platforms.

As mentioned earlier, the media plays a special role as both a business and as an expression of the community. In the main, the first information the media wants are the '5W/Hs' (who, what, where, when, why, how), plus the opportunity to publish the more salacious details or to use investigative techniques to create exclusive content. The media may also cooperate with police to inform the public or to promote senior officers' views. An extension of this role led to interesting initiative identified in fieldwork in the US, where Comcast, a media enterprise, runs the 'Everyblock' system. This system both promotes their goal of obtaining local news, and provides people with information about their local area ('neighborhood') in considerable detail. We'll return to Everyblock (and similar web-based services like Nixle) later.

On balance, it's worth sharing information about crime

The common factor that links both the desires and concerns of all three parties is the value each holds in information from the others. While this assertion is not backed by any survey, no person interviewed for this project has said that information should not be shared, or that they did not want better, clearer and timelier information. All recognised the importance of sharing in the right way and many were open to new kinds of sharing relationships. All recognised the importance of some level of reciprocity, although that level differed in both volume and time.

In order to facilitate this desire, all parties need appropriate ways to share information in ways that serve their interests and meets their respective obligations. A number of different mechanisms, which sometimes follow very different approaches to meet these needs, were observed or discussed during the fieldwork phase. Some of these are described in the next section to illustrate the available range of mechanisms.

[16] For a discussion of this topic, see Malcolm K. Sparrow, *Handcuffed: What Holds Policing Back, and the Keys to Reform*, Brookings, Washington, 2016, especially Chapters 3 and 4.

3. The mechanisms

The dimensions of sharing

The fieldwork conducted for this study has identified two principle dimensions for describing formal information sharing systems: location and working approach.

The mechanism's location—the degree to which it is located inside or outside government—is important because it will determine sources of funding, authorities for sharing, and ultimately work priorities. It will also influence the rules under which the mechanism operates and the information resources that it might draw upon. These could include classified intelligence sources, open source information or information that others are compelled to supply by law.

The working approach taken within the mechanism will fall along a continuum between information exchange and collaboration. No system observed for this study truly consists of one-way traffic. In real life, police may provide information through one route, but they will also receive information through the same or a similar one. The important distinction between the two poles of this continuum made is that information exchange does not involve an ability to develop new knowledge in a dynamic way like collaboration does. In a typical exchange situation, the government takes information in and, sometime in the future, provides information out. The inwards information might include suspicious matter reports from banks, closed circuit television images from building cameras, or reports of unusual purchases of sensitive items. 'Feedback' will come, perhaps directly in terms of alerts, or indirectly in terms of case studies or typologies.

In collaborative mechanisms, actors with shared interests work together and iteratively to solve problems. Resources are shared, information accumulates, working environments are generally close, and mutual benefits are accrued.[17] The working relationships will usually be very close, often but not always involving co-location. Indeed, the ability to bridge distances through web-based technology has significant potential, and this might both improve the ability to collaborate and reduce costs for participation in the future.

Before examining how these dimensions interact, it is worth examining the situation that lies outside this formal model.

Informal mechanisms

Of all the mechanisms, informal information sharing is the longest standing and most widely used. It is highly reliant upon personal networks, people who recognise the information needs of others, and trusted ways to share that

[17] J-P. Hatala and J.G. Lutta, 'Managing Information Sharing Within an Organizational Setting: A Social Network Perspective', *Performance Improvement Quarterly*, Vol. 21, No. 4, 2009, p. 5.

information. This trust is essential because sharers bear significant risk: there is the real potential for gain as new insights are gained and new options to solve problems come to light. There are also potential downsides. In addition to those mentioned earlier, sharers without explicit authorisation to share could face sanctions if their conduct is called into question. Sharers also bear risk as to the quality of information, which may not be verifiable before it is employed. Informal systems can also disappear when people move jobs, and suffer from degraded effectiveness until new relationships are built.

While informal information sharing may arise spontaneously and without official sanction, it is likely that such sharing will be based on an existing formal arrangement. In these cases, the informal dimension of the sharing arrangement still has significant utility: it can increase the responsiveness of the formal system, create work-arounds when the formal system does not work, and increase the richness of information gained formally.[18]

It is interesting how most of the literature reviewed for this report only refers to information sharing among government agencies. There is little research that analyses how informal information sharing might work among government, business and the community when it comes to crime: indeed, information sharing of this type may be considered highly illegitimate. Even where inter-sectoral information sharing about crime and security is described as 'informal', it still occurs within the rubric of a formal organisation.[19] That's perhaps why formal sharing mechanisms were those most encountered in this research.

Formal mechanisms

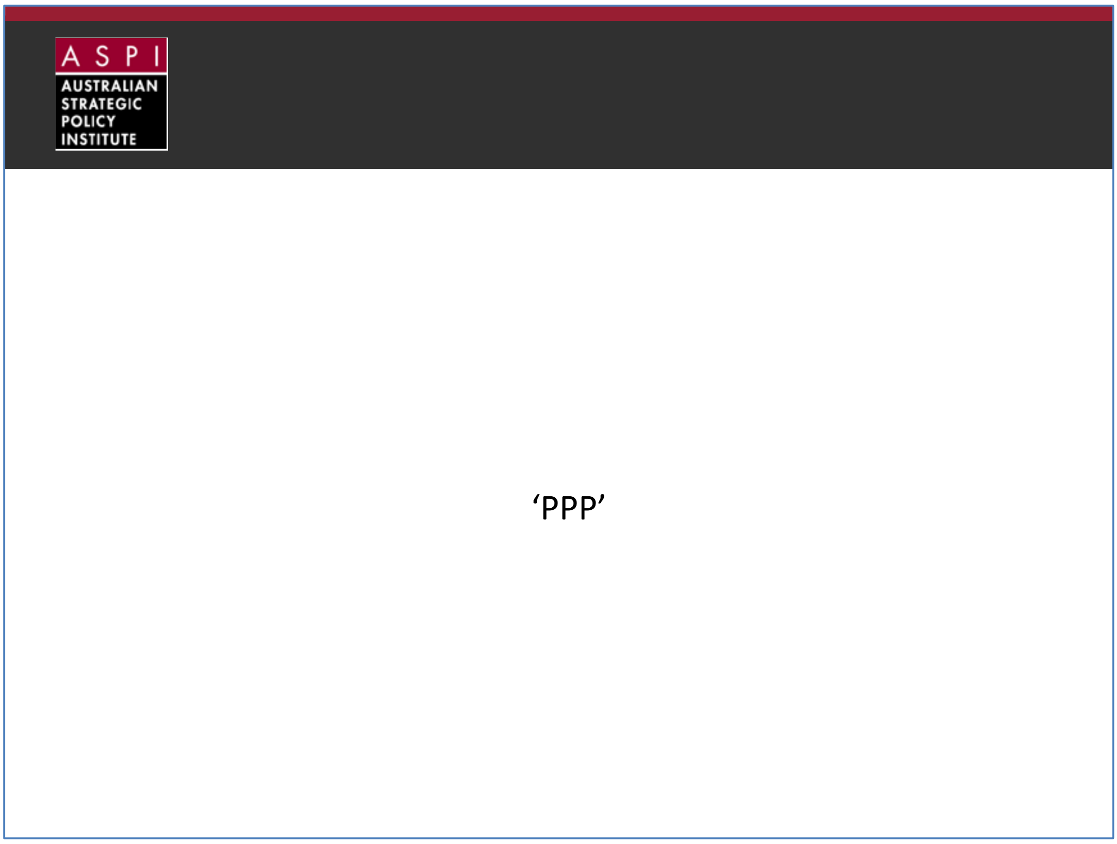
Formal mechanisms involve written agreements between the parties to share information. This agreement is drafted to not only comply with relevant laws, but to create shared expectations of each of the participants. In some cases the agreement might be used to ensure recourse in case of some form of contravention, but punitive action is unlikely to be the key motivator for an agreement. Rather, the key motivator in agreements lies in creating a trusted environment for collaboration, so that individuals without personal relationships with each other can work together.

The fieldwork phase examined 27 different formal mechanisms for sharing information about crime in general. Using the two characteristics of locations and working approach identified above, four basic kinds of formal mechanisms

[18] C. Whelan, 'Informal Social Networks within and between organisations', *Policing: An international Journal of Police Strategies and Management*, Vol. 39, Iss. 1, pp. 150-2.

[19] For example, sharing about critical infrastructure threats may occurring 'informally' within Australia's Trusted Information Sharing Network, but that networked sanctioned the initial relationships. See Australian Government, *Critical Infrastructure Resilience Strategy: Plan*, Commonwealth of Australia, c. 2010, p. 3.

can be discerned and illustrated through examples, which are described below (see Figures 1 and 2).



‘PPP’

Figure 1: A typology of formal mechanisms for information sharing

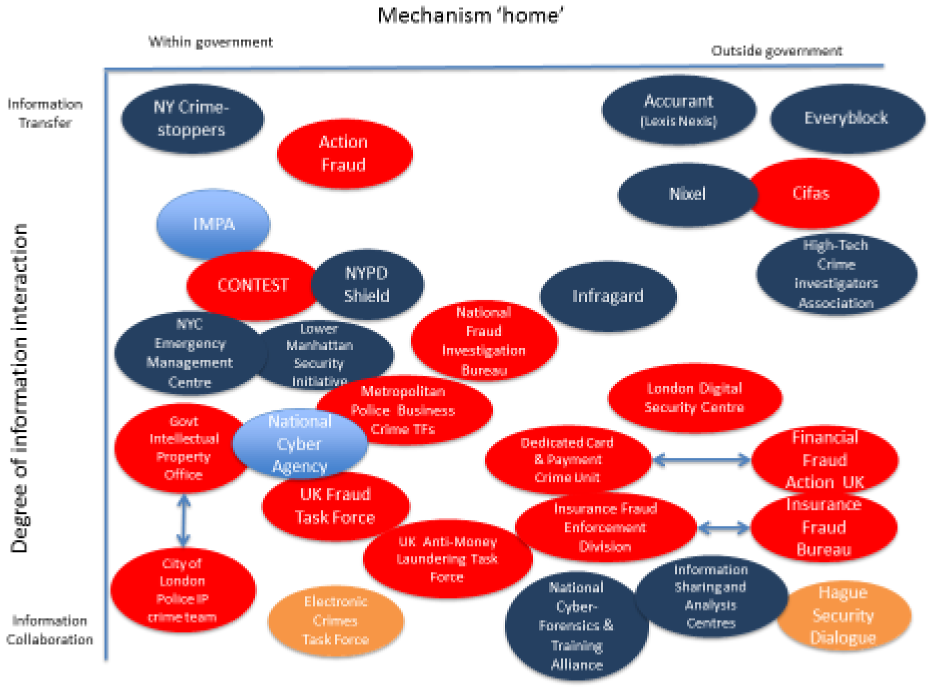

Mechanism 'home'
Within government
Outside government
Information Transfer
Degree of information interaction
Information Collaboration
NY Crime-stoppers
Action Fraud
Accurant (Lexis Nexis)
Everyblock
Nixel
Cifas
IMPA
CONTEST
NYPD Shield
High-Tech Crime investigators Association
Infragard
National Fraud Investigation Bureau
NYC Emergency Management Centre
Lower Manhattan Security Initiative
Metropolitan Police Business Crime TFs
London Digital Security Centre
Govt Intellectual Property Office
National Cyber Agency
Dedicated Card & Payment Crime Unit
Financial Fraud Action UK
UK Fraud Task Force
Insurance Fraud Enforcement Division
Insurance Fraud Bureau
UK Anti-Money Laundering Task Force
City of London Police IP crime team
Electronic Crimes Task Force
National Cyber-Forensics & Training Alliance
Information Sharing and Analysis Centres
Hague Security Dialogue

Figure 2: Information sharing mechanisms interaction/home matrix

(Note: Positioning is approximate due to the large number of organisations that overlap in given areas of the matrix. Red = UK entities; Navy blue = US; Orange = Netherlands; Light blue= Israel)

Inside government-information exchange: New York Crime Stoppers (US)

The Crimestoppers program in NY is run by a cell within the NYPD. Its basic purpose is to provide a way for members of the community to provide information anonymously, and provide cash rewards where the information is used to make arrests. While the unit is part of the NYPD Detective Bureau, the reward money is provided by the NYPD Foundation. This creates and arm's length relationship between the taxpayer and those who receive the rewards.

Outside government-information exchange: Everyblock (US)

'Everyblock' (www.everyblock.com) is a web-based information service that operates in a number of major US cities. This service is provided by media corporation Comcast, and started as a way for local media organisations to remain abreast of events. It was also used as a way of providing local content to users at a time when news outlets were being amalgamated into larger units.

In today's format, Everyblock has also become a platform for police 'Open 311' information (non-emergency requests for assistance), council notices like road closures and building permits, and events like neighbourhood meetings and block parties.

Everyblock is managed as a business unit of Comcast. Most control is maintained locally by Comcast local media outlets, who maintain a moderating function on the bulletin board. The company is able to monitor direct uptake and use very accurately, as well as identify where its content is used by others.

Inside government-collaborative: Electronic Crimes Task Force (Netherlands)

Formed in March 2011, the Electronic Crimes Task Force (ECTF) is a partnership between the Dutch National Police, the National Public Prosecutor's Office, and a number of financial institutions.[20] This unit is hosted within the National High Tech Crime Unit, a part of the Central Criminal Investigations Division, but its work is guided by a supervisory committee.

This committee is chaired by a Deputy Police Commissioner and includes the National Cyber-Crimes Prosecutor, the Head of the High-Tech Crime Unit, representatives of all members (usually the head of anti-fraud and compliance) and a representative from the Ministry of Security and Justice. The committee meets every eight weeks. It does not provide operational direction to the Task Force, as this remain a police responsibility.

The ECTF has a complement of around 13 people, drawn from the National Police, business and other government partners. All ECTF partners sign a covenant, which sets out the role, legal basis, expectations and responsibilities of each member. Participants also agree to bear all costs associated with their participation, and assign at least one person to the ECTF. The actual office itself is a small room with 10 workstations.

The information shared within the ECTF is case information, in the form of responses to enquiries about a particular customer, transaction or account. The information is only shared within the boundaries of the ECTF.

This system requires a high level of trust in both the operational model and the individual involved. The task force is able to short-cut the usual processes, which can take months, and to respond to emerging threats and methods. Indeed, the ECTF prides itself on looking for the new methods as it feels best place to identify and analyse these.

Outside government-collaborative: National Cyber-Forensics and Training Alliance (US)

The National Cyber-Forensics and Training Alliance (NCFTA) is a US public-private partnership specialising in countering cyber threats through information sharing amongst and across industry and government within a trusted environment. Founded in 2002, the NCFTA is focused on identifying, mitigating, and neutralizing cyber threats globally through three main programs: Cyber Financial Program (CyFin), Brand & Consumer Protection Program (BCP), and Malware & Cyber Threats Program (MCT). The NCFTA is located within the FBI's Internet Crime Complaint Centre (IC3) in West Virginia.

[20] The full non-government membership list is: ABN-AMRO, Rabobank, ING, SNS Bank, the Dutch Bankers Association, and the International Cards Association.

The NCFTA was established as a 501 (c) (3) nonprofit corporation with a board of directors drawn from various sectors. It operates with a complement of approximately 100 people, about half of whom work for the NCFTA, with the remaining team members coming from US and foreign law enforcement agencies and various industries. The NCFTA also has an extensive network of affiliates and member organisations in the US and overseas, and is closely associated with the FBI's Cyber Initiative and Resource Fusion Unit.[21] Its resource base is not publicly disclosed.

The NCFTA operates by conducting real-time information sharing and analysis with subject matter experts (SME) in the public, private, and academic sectors. Participants in the NCFTA must sign a confidential membership agreement to participate, and the alliance has strict non-disclosure requirements.

The type of information shared is case-based. The NCFTA uses communications platforms such as listservs, working groups, and peer calls to discuss which issues are being seen in various industries and how best to address them. The NCFTA also utilises its Internet Fraud Alert (IFA) system to report stolen account credentials discovered online.

The NCFTA enables close contact between private sector cyber and intelligence experts and experienced law enforcement officers to promote responsiveness, security and collaborative approaches to problem solving.

A model worth noting: Financial Fraud Action UK and the DCPCU (UK)

One last model worth noting belongs to the 'outside government-collaborative' sector, but it also straddles the 'inside government' sector due the unique policing arrangements.

Financial Fraud Action UK (FFA UK) is responsible for leading the fight against fraud on behalf of the UK payments industry. As such, the membership of FFA UK includes banks, card issuers and card payment acquirers in the UK. Its focus is on non-competitive fraud issues. This sees FFA UK involved in an industry strategic threat management process, managing industry intelligence sharing about fraud (the Financial Fraud Bureau), expert security assessments, and outreach including public affairs and awareness. FFA UK has close information sharing relationships with National Crime Agency, National Fraud Intelligence Bureau, and the Dedicated Card and Payment Crime Unit (DCPCU).

DCPCU is a collaborative arrangement between the Metropolitan Police Service, the City of London Police, and FFA UK. Importantly, the DCPCU itself is not part of a police force, but a collaborative arrangement between the three partner groups. It is managed by a board, and receives administrative support from the

[21] 'The NCFTA: Combining Forces to Fight Cyber Crime', Federal Bureau of Investigation, 2011, available: https://www.fbi.gov/news/stories/2011/september/cyber_091611.

City of London Police. It is operationally independent of all other organisations and agencies.

DCPCU has around 39 people, and FFA UK has around 29 people. Both are fully sponsored by the banking industry, with the DCPCU's funding being managed through FFA UK, in the order of around GBP£4m annually. The DCPCU is accommodated with FFA UK in adjacent offices.

Case information is the basis of sharing within this arrangement. Intelligence briefs or information about individuals or accounts is provided by banks or FFA UK to DCPCU. DCPCU has fraud investigators and liaison officers from industry as well. DCPCU also receives police information from other agencies.

This mechanism provides for very close relationships between industry and government. However, it was described as uncontroversial because its actual structure and practices allow the police unit to be at arm's length from individual companies and operationally independent. It is also clear that the arrangement adds additional resources to policing, as well as a home for specialised investigators.

These mechanisms are only a sample of those studied during the fieldwork phase. Further examples can be found in the country annexes attached to this main report.

4. Factors influencing inter-sectoral information sharing about crime

The country annexes covering Israel, the United Kingdom, the Netherlands and the US (Annexes A-D) also describe the factors that enable and constrain information sharing between government, business and the community within those jurisdictions. The fieldwork found that all the nations visited had different but broadly similar abilities to share information, albeit with authorities that varied even between like agencies. All had access to similar technologies for sharing. The practices and mechanism were, however quite different among these four nations.

This final section draws conclusions for information sharing about crime in general, with a focus on the factors that enable and constrain inter-sectoral sharing. These conclusions are based on the discussions with experts involved in the field (see Annex E), and are tempered by the findings of literature examined for this project.

Factors enabling information sharing

Other researchers have identified many different factors that promote information sharing among different sectors. Robinson and Disley identify economic incentives stemming from cost savings, and incentives stemming from the quality, value, and use of information shared as the two primary enablers.[22] Yang and Maxwell examine three inter-related contexts for information sharing: interpersonal, intra-organisational and interorganisational. At the interpersonal level, socialisation is both an influential factor and a process that facilitates information sharing, especially explicit knowledge and tacit knowledge, between individuals. However, the information-sharing behaviors become more complicated when individuals operate within the intra-organisational and inter-organisational levels. Understanding the enabling factors at these levels requires an analysis of culture, incentive systems, information technology, belief systems and political and legislative support.[23] LeBuef and Pare emphasise personalized factors such as direct human contact, trust in people and processes, and support as their main promoting factors.[24] Research for this report tends to support the broad findings of these scholars, but offers a slightly different emphasis and a completely different primary reason for sharing.

Indeed, research for this study found the primary reason why the three groups share information about crime is a shared sense of need. This is especially so in situations where business sees a chance to reduce their losses and other risks by cooperating with government agencies. Government agencies also acknowledge their shortcomings and see value in cooperation with business, and are prepared to create suitable trusted mechanisms.

It is also important for government agencies to see the community as an opportunity to collaborate in solving crime, and not only as a partner for information exchange. Admittedly, most of the current collaborative activity revolves around neighbourhood crime, which is not necessarily about organised crime. Despite that, it is possible to see how web-based technologies could enhance government-public collaboration, especially for reporting the signs of organised crime such as sales of counterfeit or illicit goods. Web-technologies also have potential to deal with the challenges for government posed by the scale of information and provide necessary contact points required for public involvement.

Shared needs, threats and goodwill are necessary for information sharing, but insufficient. In addition, information sharing must be positively enabled through political support, resources and legislation. Without such support, government agencies may lack the legitimacy to share, and the ability to assign people and processes to create and maintain an effective and legal system. The needs of both

[22] Robinson and Disley 2010, p. 16. In addition to these 'high' importance incentives, they also identify 'medium' and 'low' importance incentives including interpersonal trust, autonomy for participants with company support, and direct economic incentives like subsidies.

[23] Yang and Maxwell 2011, p. 169. Interestingly, they find intra-organisational sharing more problematic than intra-organisational.

[24] M-E LeBeuf and S. Pare 'Police Information Sharing in Canada: Balancing Security, Efficiency and Collaboration, Royal Canadian Mounted Police, Ottawa, 2005, p. 23.

business and the community also be factored in, as these groups can help generate support and must see value in cooperation. That's especially so when participation in information sharing costs money, so businesses in particular must gain value worth the cost.

Mechanisms allowing businesses to share incriminating or potentially damaging information must also be devised to enable sharing. These might include immunities, delayed prosecutions, voluntary restitution or self-corrective action. Safeguards would also be needed, and may include protections from secondary uses of the information, for example, in tax proceedings. Regardless of the forms taken, devising such mechanisms will present a difficult balancing act for all concerned, but at least having some ways to encourage such disclosures will create conditions for voluntary information sharing about the most sensitive matters.

Of course, information sharing is not always voluntary. Obligation, such as those imposed under AML/CTF regimes, also make sure information is passed from business to government. The result is not always economical, for the useful reports used are said to be small proportion of the total. Improving the ability to mine information provided in bulk should therefore be a priority for government agencies, so they can get more from what they hold.[25] Without addition attention and use, obligatory reporting appears costly and contains risk. That risk can materialise when unexploited data holdings are found to contain important pieces of information that might have prevented a crime.[26] The often slow feedback involved in this type of relationship tends to detract from the value of participation by businesses in particular.

Smart structures also promote information sharing, and a number of these were studied during fieldwork. When enabled by legislation, structures (and their enabling agreements) provide the forum and details of participation that legislation will not provide. But even lacking legislation, agencies and businesses can enter meaningful partnerships based on existing authorities or even general measures that help to fight crime.

The Dutch ECTF is a good example of such an arrangement. Creating arms-length relationships between business and law enforcement has also helped to create high degrees of collaborative information sharing in both the US and UK, in fields including cybercrime and fraud. In terms of the latter, the sponsorship of police units by business associations has added particular value: additional resources are created for law enforcement agencies, highly trained investigators are retained in units with a single focus, and the particular needs of an industry can be met expeditiously. While private sponsorship of policing is highly

[25] Discussion with Australian government official, 23 May 2016.

[26] For a significant criticism concerning the inability to aggregate and make sense of existing information holdings by government, see 9/11 Commission 2004, p. 353-7.

controversial in other contexts, the UK's approach does not appear to attract any controversy.

Structures also help to create trust. As mentioned earlier, there is some thought that interpersonal relationships are needed to establish the level of trust needed to create effective sharing mechanisms. In many of these cases observed, it would be fair to assert that the mechanism came before the relationship, and so information was shared before the trust was developed. In this way, good structures—based on agreed and known rules, secure communication, and ultimately value—can create the conditions that allow information sharing to prosper.

On the other hand, it seems that when organisations become too large the ability to exchange sensitive information can go into decline. In a few of the mechanisms observed, large groups of unvetted people do not create good conditions for sharing. That does not make such groupings useless or dangerous—it just limits the utility of using large groups. On the up-side, people will meet through these arrangements, create relationships and find new ways to share the information they need. Web-based technology, which requires members to be accepted, can also promote good information sharing among large groups. But the sensitivity of information shared in such broad-based forums is likely to be low, untimely and potentially broadly focused.

At the opposite end where informality rules, low levels of public scrutiny and oversight can also promote information sharing. The lack of security can effectively create 'space' for information to be shared or traded, which raises concerns over legality, fairness and security. In today's climate, where such arrangements are often considered illegitimate, active steps might actually be taken to inhibit such information sharing.

Factors inhibiting information sharing

Of the main factors inhibiting information sharing, legislation is often cited first and identified for two reasons. Firstly, privacy laws and the desire to avoid 'criminalising' legitimate daily activity can combine at different times to inhibit sharing. This is the concern about 'big brother', but the challenge is also reflected in the sheer volume of possible data that both business and government agencies have, and the public can provide. Anti-trust laws were also cited as a legal inhibitor in some countries. In these situations, companies might not be allowed to share information directly and will need a third party such as a professional association or law enforcement facilitator, or enabling legislation such as the US PATRIOT Act, to manage that difficulty.[27]

[27] One interlocutor spoke highly of the USA PATRIOT Act Sections 314(a) and 314(b), which helps law enforcement identify, disrupt, and prevent terrorist acts and money laundering activities by encouraging further cooperation among law enforcement, regulators, and financial institutions to share information regarding those suspected of being involved in terrorism or

Legislative complexity is the second reason. In some countries, it can be very hard to identify all of the legislation that impacts upon information sharing, even when a guide is produced to provide a one-stop reference for sharing. That's because training is an additional piece of the puzzle, and that may not be provided before a person is brought into an information sharing mechanism. Still, this inhibitor is solvable and local facilitation measures can help.

Poor quality information, whether it be too hard to digest or not valuable enough to justify the costs of sharing was another inhibitor. In some of the larger mechanisms with thousands of members, the information passed is often no better than media reports. In other systems, unrefined information might simply swamp those with a small capacity to deal with it.

The lack of a two-way street for information sharing might be an inhibitor. This occurs especially in information exchange situations: there tends to be a long delay between information moving to government from business or the community, and the government's return response to that information. This situation was especially noticeable in the banking sector, where formal requirements to share information led to an excess of information being provided to government, and frustration at the time taken for government to provide updated information about criminal trends and methods back to the banks. According to some interlocutors, this situation discourages active assistance and discrimination by business because the return is neither timely nor specific enough to warrant an investment in improving the quality of their sharing. Others point to the need to use the data better so those providing information see more value for their contribution.

The cost vs. return factor plays in other ways. Some businesses may be reluctant to participate in sharing mechanisms that do not provide immediate returns for them. Others may lack the scale and resources to participate, especially where meetings and committees are required. This means small and medium sized companies (not to mention the general public) can actually be excluded from participating in information sharing. Yet when efforts are made to include those with more limited resources, a paradox arises because the mechanism is less trusted, and the information is less tailored and less 'special'. Cost also figures in government calculations too.

In some countries, distinctions between 'criminal' and 'national security' intelligence remain or have only recently been removed. This creates challenges for sharing these two related types of information as systems because the systems in place do not necessarily allow easy movement between the domains. This is particularly so because security clearances for people and information systems take time and money to change. In the US, formal procedures are required to share information between these domains and some believe that

money laundering (see https://www.fincen.gov/statutes_regs/patriot/index.html?r=1&id=314#314).

such sharing cannot take place in any case.[28] There remains some tension between the standard 'need to know' principle for information sharing and the emerging norm of a 'duty to share'. This tension becomes evident when it remains up to the individual to know who actually needs the information at hand, and means that established relationships are really the only ones serviced.[29]

The self-conception of law enforcement agencies, which places primacy on arrests and prosecution, can inhibit information sharing. In this frame, sharing information can actually impede their ability to prosecute because a 'premature' act could result in a mistrial or miscarriage of justice. It is this concern that often leads government agencies to hold onto valuable information until court proceedings are complete. This inhibition means other criminals using the same methodology may continue to exploit a vulnerability for some time after the initial discovery.

Of all of the factors, most of those interviewed for this project agreed that 'culture' was the main inhibitor. What culture actually meant was more difficult to unpack. For some, the 'culture of secrecy' was the key concern because it prevented relationships from forming in the first place. Many in government and business subscribe to this culture for a good reason, as information about crime is highly sensitive and can do harm to society if released in uncontrolled ways. While true, this reason does not account for every situation where sharing would be possible but does not occur, such as in the cases relating to countering money laundering or fraud methodologies. For others, a culture of 'information is power' was dominant, even if this was harder to pinpoint with the research method used.

Yet culture can also be seen as an excuse. In a number of instances, a lack of understanding, complicated rules, costs and an absence of leadership can also explain the absence of sharing. That means the search for reasons why information is not shared—and options for how this act can be improved—needs to take the widest possible scope.

[28] A view (now dated) expressed in National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 2004, p. 79, available: http://www.9-11commission.gov/report/911Report.pdf. Still, information gained through electronic surveillance under 50 U.S. Code § 1806 – 'Use of information' cannot be disclosed to law enforcement 'unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General' (section b).

[29] See Cabinet Office, 'Government Security Classifications', HM Government, April 2014, which says officials need to share information proactively (para 8) and their subsequent requirement to share only with those who have a 'need to know' (para 9). Note the impassioned plea for officials to adopt a 'need to share' approach contained in 9/11 Commission 2004, p. 417.

Conclusion

This four-nation survey of information sharing about organised crime, which was conducted with the support of the 2015-16 Donald Mackay Churchill Fellowship, was an opportunity to examine a number of different structures, processes and cultures of relevance to Australia. The systems studied varied greatly: they included the formal and informal; the impersonal and intimate; and the technology-enabled and 'old school'. All were different, and all had their place in their particular context.

The range of interviews undertaken covered all three actor groups in the 'triangle of shared interest', and the time available during the Fellowship allowed for some in-depth discussions about their respective views of the risk, utility and cost of their existing arrangements. While these interviews showed different perspectives on information sharing, they also showed strong support for the concept and offered different approaches to doing so.

This research found both upsides and downsides to information sharing about crime. There were many risks for those sharing and these were often considered first. Still, it is clear that sharing must occur. That's because the scale of the challenge posed by organised crime—and the speed, reach and depth of penetration that the internet enables—means information sharing is critical for all three groups.

Finding optimal ways to achieve sharing is therefore a critical task, but it was clear from this research that no single way is 'the best'. Legislative factors, resources, threat and national style all played a role in identifying the preferred mode. What allowed that mode to be analysed were the common features of these information sharing systems: the information shared (case based or bulk data), the approach taken (exchange or collaborative), and the location (inside government or inside business). These attributes can be effectively combined to scope the field, and identify different candidates for new system design.

Yet while the mechanisms differed, the major inhibitors and enablers of information sharing in these systems were relatively consistent across the national jurisdictions. This research found that the shared need was perhaps the greatest enabler of information sharing, which means building this sense of common purpose will be a vital step in the design and implementation of any system. Creating a trusted system, which in turn enables legitimate information sharing, seemed to precede and transcend interpersonal trust, which is a factor others have seen as critical to sharing. At the risk of channeling old movies, 'build it (sensibly) and they will come' might be the best guide for information sharing system designers.

While legislation was often considered the greatest inhibitor, most participants described a reasonably enabling environment for sharing. Instead, much of the friction could be explained by culture. But this concept needs to be unpacked: are we talking about leadership, ways of working, or education? Again, attention to all of these is important and no one intervention is likely to overcome the inhibitions faced by those entrusted with sensitive information.

The next question for this research is, 'so what for Australia'? The potential ways to do that will be canvassed in Part 2 of this project. This work will aim to identify new approaches to thinking about information sharing, suggest legislative reforms, describe some possible structures, and identify education needs to bring the triangle of shared interests together in Australia, so they may share information about organised crime for the right reasons, and in the right ways.

Annexes

A. Israel
B. United Kingdom
C. The Netherlands
D. The United States
E. Meetings

References

Note: All internet links were live on 1 May 2016

Abdollah, Tami. 'U.S. Homeland Security department to share cyber threat data', Canadian Underwriter, 18 March 2016, available: http://www.canadianunderwriter.ca/insurance/u-s-homeland-security-department-to-share-cyber-threat-data-1004082255/.

Accenture. 'Creating revenue from customer data', available: https://www.accenture.com/hk-en/insight-data-monetization-summary.aspx.

Agencies. 'Ten arrested in Netherlands over bitcoin money-laundering allegations', *The Guardian*, 20 January 2016, available: http://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy

Attorney General's Department. *National Organised Crime Response Plan 2015-18.*

Australian Crime Commission (ACC). *Organised Crime in Australia 2015*, Commonwealth of Australia.

Australian Government. *Critical Infrastructure Resilience Strategy: Plan*, Commonwealth of Australia, n.d.

Ayling, J. 'Going Dutch? Comparing Approaches to Preventing Organised Crime in Australia and the Netherlands', Regnet Research Paper, Australian National University, Canberra, 2013.

Barnett, Gary D. 'InfraGard: An unhealthy Government Alliance', available: http://fff.org/explore-freedom/article/infragard-unhealthy-government-alliance/.

Cabinet Office. 'Government Security Classifications', HM Government, April 2014.

Carter, J.G. 'Inter-organizational relationships and law enforcement information sharing post September 11 2001', *Journal of Crime and Justice*, Vol. 38, No. 4, 2015.

Chermak, S; J. Carter, D. Carter, E.F. McGarrell, and J. Drew. 'Law Enforcement's Information Sharing Infrastructure: A National Assessment', *Police Quarterly*, Vol. 16, No. 2.

Connery, D; C. Murphy and H. Channer. 'Web of Harms: Serious and Organised Crime and its impact on Australia's interests,' Australian Strategic Policy Institute Special Report 81, Canberra, 2015.

Department of Homeland Security. 'Local Anti-Terrorism Information and Intelligence Sharing: Overview', n.d., p. 1, available: https://www.hsdl.org/?view&did=765456.

Department of Homeland Security, 'NIPP 2013: Partnering for Critical Infrastructure Security and Resilience', 2013, available: https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

Dix, Robert B. Jr. 'Blog: Situational Awareness Will Inform Risk Management Decision Making', 5 May 2016, available: http://www.afcea.org/content/?q=Blog-situational-awareness-will-inform-risk-management-decision-making#sthash.9m7Gx84T.dpuf.

Domestic Security Alliance Council. 'Member Benefits', available: https://www.dsac.gov/about/dsac-member-benefits.

DutchNews.nl. '200 questioned in Dutch-led crackdown on 'money mules', 1 March 2016, available: http://www.dutchnews.nl/news/archives/2016/03/european-police-target-money-mules-holding-e7-5m-in-bank-accounts/

European Union Migration and Home Affairs. 'Information exchange', available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/information-exchange/index_en.

FBI. 'InfraGard: A partnership that works', 2010, available: https://www.fbi.gov/news/stories/2010/march/infragard_030810.

Fijnaut, C. 'The innovative containment of organized crime problems in Amsterdam's inner-city, 1996-2015', n.d.

Government of the Netherlands. 'Public Administration Act (Bibob) will be extended to intensify the fight against organized crime', February 2011, available: https://www.government.nl/latest/news/2011/02/21/public-administration-act-bibob-will-be-extended-to-intensify-the-fight-against-organized-crime

Government of the Netherlands. 'New Public Administration Act effective as well as celebrating an anniversary, June 2013, available: https://www.government.nl/latest/news/2013/06/24/new-public-administration-act-effective-as-well-as-celebrating-an-anniversary.

Hatala J-P. and J.G. Lutta, 'Managing Information Sharing Within an Organizational Setting: A Social Network Perspective', Performance Improvement Quarterly, Vol. 21, No. 4, 2009.

Healthcare and Public Health Sector Coordinating Council. 'Comprehensive Charter' (Version 1.5), available: https://www.dhs.gov/sites/default/files/publications/Healthcare-SCC-Charter-2014-508.pdf.

HM Government. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010.

iHLS. 'Reporting Crime With Your Smartphone', 2 December 2015, available: http://i-hls.com/2015/12/reporting-crime-with-your-smartphone/.

iHLS. 'Civic Apps: Can They Help Fight Crime?' September 2014, available: http://i-hls.com/2014/09/civic-apps-can-help-fight-crime/.

Kleemans E. R. and W. Huisman. 'Multi-agency approaches in "crimogenic" settings: the case of the Amsterdam Red Light District', *Crime, Law and Social Change*, 64:4-5, 2015

Kruisbergen, E.W; D. De Jong and E.R. Kleemans, 'Undercover Policing: Assumptions and Empirical Evidence', *British Journal of Criminology*, 2010.

von Lampe, K. 'The Concept of Organized Crime in Historical Perspective', 1999, available: http://www.organized-crime.de/lauhtm01.htm.

LeBeuf, M-E and S. Pare. 'Police Information Sharing in Canada: Balancing Security, Efficiency and Collaboration', Royal Canadian Mounted Police, Ottawa, 2005

Moss, Randolph D. (acting Assistant Attorney General). 'Legal Effectiveness of Presidential Directive, as Compared to an Executive Order', 29 January 2000, available: http://fas.org/irp/offdocs/predirective.html.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*, 2004, available: http://www.9-11commission.gov/report/911Report.pdf.

National Crime Agency. *Strategic Assessment of Serious Crime*, June 2015.

National Security Council. 'Transnational Organized Crime: A Growing Threat to National and International Security', available: https://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat.

Netherlands Police Agency. 'Agreement on Collaboration and Information Exchange: Electronic Crimes Task Force (English Version)', 2011.

Obama, President Barak. 'Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security', 2011, available:

https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

Obama, President Barak. ‘Empowering Local Partners to Prevent Violent Extremism’, August 2011, available: https://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

Obama, President Barak. ‘National Strategy for Information Sharing and Safeguarding’, December 2012, available: https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

Obama, President Barak. ‘Executive Order—Promoting Private Sector Cybersecurity Information Sharing, 13 February 2015, available: https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Obama, President Barak. ‘Executive Order—Establishment of the Federal Privacy Council’, 9 February 2016, available: https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.

OECD. ‘Information exchanges between competitors under competition law’, 2010.

Plecas, D.; A. McCormaick, J. Levine, P. Neal and I. Coen. ‘Evidence-based solution to information sharing between law enforcement agencies’, Policing: An international Journal of Police Strategies and Management, Vol. 31, No. 1, 2011.

Raine, L. and M. Duggan, ‘Privacy and Information Sharing’, Pew Research Center, 14 January 2016.

Reporters Committee for Freedom of the Press. ‘”InfraGard” lets FBI disclose sensitive information to select few’, 2002, available: http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-winter-2002/infragard-lets-fbi-disclose#sthash.rIiKReLs.dpuf.

Robinson, N. and E. Disley. ‘Incentives and Challenges for Information Sharing in the Context of Network and Information Security’, European Network and Information Security Agency, 2010

Sparrow, M.K. *Handcuffed: What Holds Policing Back, and the Keys to Reform*, Brookings, Washington, 2016.

Stanley, J. ‘The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society’, American Civil Liberties Union, 2004.

‘Summary: CT Infobox 10 years’, c. 2015.

UK Home Office. ‘National Support Framework: Information Sharing for Community Safety’, HM Government, 2010.

US Department of Homeland Security. ‘Privacy Impact Assessment for the Automated Indicator Sharing (AIS)’, DHS/NPPD/PIA-029(a), 16 March 2016.

US Department of Homeland Security. ‘NIPP 2013: Partnering for Critical Infrastructure Security and Resilience’, available:

https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

US Embassy Tel Aviv. 'Israel: Promised land for Organised Crime?', 15 May 2009.

Sales, N.A. 'Mending Walls: Information Sharing after the PATRIOT Act', *Texas Law Review*, Vol. 88: 2009-10,

Yang T.M. and T.A. Maxwell, 'Information Sharing in Public Organisations: A literature review of interpersonal, intra-organisational and inter-organisational success factors', *Government Information Quarterly*, 28, 2011.

Whelan, C. 'Informal social networks within and between organisations', *Policing: An International Journal of Police Strategies and Management*, Vol. 39, Iss. 1.

Abbreviations

ACC	Australian Crime Commission (Australia)
AML/CTF	Anti money laundering and counter-terrorism financing
BCP	Brand & Consumer Protection Program (US)
BIS	Department for Business, Innovation and Skills (UK)
CIPFA	Chartered Institute of Public Finance and Accountability (UK)
CyFin	Cyber Financial Program (US)
DCPCU	Dedicated Card and Payment Crime Unit (UK)
ECTF	Electronic Crimes Task Force (Netherlands)
FBI	Federal Bureau of Investigation (US)
FCA	Financial Conduct Authority (UK)
FFA UK	Financial Fraud Action United Kingdom
FIU	Financial intelligence unit
IFA	Internet Fraud Alert
IFED	Insurance Fraud Enforcement Department (UK)
IP	Internet protocol
ISAC	Information Sharing and Analysis Centres (US)
LDSC	London Digital Security Centre (UK)
MCT	Malware & Cyber Threats Program
MOPAC	Mayors Office for Policing and Crime (UK)
NAVCIS	National Vehicle Crime Intelligence Service (UK)
NCTFA	National Cyber-Forensics and Training Alliance (US)
NFIB	National Fraud Intelligence Bureau (UK)

NFP	Not for profit
PII	Personally identifiable information
PPP	Public-private partnership
RART	Regional Asset Recovery Unit (UK)
RFT	Regional Fraud Team (UK)
ROCU	Regional Organised Crime Unit (UK)
SME	Small-medium enterprise
SME	Subject matter expert
UK	United Kingdom
US	United States of America

Annex A: Israel

Context

Organised crime has been described as a 'later comer' to Israel. It took successive governments nearly a decade after a landmark 1971 newspaper investigation to agree that organised crime—or 'organised criminality' to use the locally-acceptable term—was a problem. Even then, the operating modes and defining characteristics of organised crime were not accurately assessed for another twenty years.

Despite this slow official start, many characteristics of Israeli organised crime have been clear for some time. These include its 'Mafioso style' whereby 'crime families' dominate territory through corruption, precipitous violence and high levels of international connectivity. These factors are both aided by the patterns of immigration into Israel, the presence of significant ethno-religious enclaves that are hard for law enforcement to penetrate, and the large Jewish presence in countries like the USA and Russia.[30]

The activities and enterprises of Israeli organised crime reflect both 'usual' activities and some created by local conditions. Israel is a significant consumer market for drugs and a transit point to other countries. It is also a target for money laundering, and its desire to attract legitimate Jewish capital from across the world masks some illegitimate funding at the same time. Human trafficking for prostitution has been another noted concern, which is often facilitated by smugglers. These smugglers are not choosy with their cargo, so they may smuggle drugs or other contraband one day, and weapons and explosives the next.

Tough economic conditions, different restrictions and taxation arrangements also create opportunities for crime. Interlocutors for this project described how tight credit conditions imposed by banks was encouraging some businesses to obtain 'grey market' finance, while unregulated donations to politicians can influence political behavior. Gambling is a major crime industry because it is illegal in Israel, while rackets including value-added tax avoidance in the grey market and even one involving bottle recycling have been reported. Crime families also fight for both money and honour in Israel, which means about 50% of the nation's murders each year are attributed to organised crime activity, according to a leading Israeli criminologist.

Overall, moral panic and high levels of politicization but low levels of political attention due to the focus on state-based threats and domestic terrorism marked the early period of Israeli engagement with organised crime. It took a shocking incident of public violence in 2003 (and perhaps a lesser degree of security

[30] For one assessment of these impacts, see US Embassy Tel Aviv, 'Israel: Promised land for Organised Crime?', 15 May 2009.

threat) to galvanize action. Major legislative innovations included laws against money laundering (2001) and organised crime (2003). Specific resources for witness protection were provided in 2006. A 'map' of organized crime groups in Israel was completed in 2006. Significant new resources were given to the INP in 2008 to create a stronger national approach toward defeating organised crime, including through the formation of a specialised police unit, known as Lahav 433.

In the Israeli system, the Israel National Police (INP) is the 'lead agency' against organised crime, and it works closely with the prosecutors to develop and manage major cases. There are a number of other specialised agencies that support the effort, including the Tax Authority, the anti-money laundering agency IMPA and the Ministry of Public Security. The security service, especially the Israeli Security Agency, play a major role in other aspects of crime fighting and information, especially on counter-terrorism.

The new INP Chief has a major focus on crime prevention, and he's cast countering money laundering as a key component of this because removing money and assets from criminal enterprises makes them more vulnerable to police activity.

Sharing information about financial crime

The financial intelligence unit, Israel Money Laundering and Terror Financing Prohibition Authority (IMPA) was established in 2002. Its role is to produce financial intelligence about money laundering and terrorist financing: but its placement as a 'buffer' between the financial institutions and the police is important. Given the large number of transactions each day, and the large number of 'unusual' transactions that do not merit investigation (about 95% of all matters reported), providing reports straight to the police was a real privacy concern for Israel's banks customers. IMPA was designed with that concern in mind.

IMPA therefore does not have a regulatory or investigation function. Its job is to collect 'unusual transaction reports': reports of large money movements domestically and internationally. It also analyses incidental financial intelligence from the private sector, other government agencies and the public.

IMPA has very tight rules about information sharing. Authorized agencies are listed, and where there is a suspicion of a crime the INP is informed. In a recent innovation, IMPA, Tax and INP now work closely together in a fusion centre to exchange information and target high priority criminals through their finances. Israel has laws requiring mandatory reporting of suspected terrorist financing.

IMPA compliance officers work with their client businesses to explain processes, and this often promotes informal sharing about methods and risks. In addition, IMPA publishes money laundering and terrorist financing methodologies, but these are long delayed to protect the integrity of court cases.

Educating judges, prosecutors and police about financial crime was considered a critical activity because the general level of understanding of the crimes and the evidence is low. So too is broadening the range of industries who must comply with 'know your customer' and unusual transaction reporting regulations.

Counter-terrorism

Israel does not have a written counter-terrorism strategy, but this is a vital national priority. Interlocutors described some of the key information sharing challenges within government, including the range of departments now involved in CT—'newcomers' who do not have a grounding in national security.

The Counterterrorism Bureau acts a regulator of CT activity on behalf of the Prime Minister. Its functions include checking others, looking for gaps, adjudicating on requests by the various services, and issuing travel warnings. It is a small team, with a focus on intelligence cooperation and facilitating political control of major incidents. This office has no contact with businesses, and this is left to the intelligence agencies.

The Israeli Security Agency (Shabak/Shin Bet) is an information gathering agency with extraordinary powers to protect the state. Its methods for collection are extensive and the source of approvals to use these means rest with the Prime Minister (with oversight from the Attorney-General and judicial mechanisms), unlike the police who need warrants. As a result of these powers, and the paramount objective of maintaining security, the ISA has a limited ability to share information with any other agency and these are described in regulations (for example, sharing with the police is easier than with social service departments or with business). Employees cannot divulge information without approval. It has a section that interacts with business by approving information technology before use in government services.

Cyber security

Israel is undertaking a new effort in cybersecurity, involving an amalgamation of existing civil and military organisations under a new authority within the Prime Minister's Office. While its information sharing arrangements for the National Cyber Authority (NCA) have yet to be formalized, a strong role for industry—including major international technology firms—is envisaged. But a formal mechanism is not considered likely, as 'everyone knows everyone' (this refrain was constantly reinforced in discussions). The needs and capacities of smaller firms have not been broached yet, although support for Israel's 'golden eggs' of innovative start-ups is envisaged. International information sharing is considered very important.

So far, the Israeli government has been approaching the nation's cybersecurity needs by sector. The next step is to create a hub for information technology (and security) that will promote government-military-business-education cooperation.

Business perspectives about information sharing

Business groups see information sharing as a one-way street in Israel. They rely heavily on public messaging and their informal networks. But as others have noted, corporations hold more information today than government, and this is a real concern in Israel.

The ability to unlock this information is constrained by anti-trust laws. While these laws are designed to prevent collusion in the marketplace, they serve to prevent direct information sharing among business at the same time. Laws to address this situation, perhaps in the form of the US Patriot Act Sections 314(a) and 314(b), were recommended by one businessperson.[31]

Two firms involved in the private security and intelligence business said they do not participate in any formal information sharing arrangements with the Israeli government. While much of the work of one is done off-shore, they provide security advice and protective services to major corporations who deal within Israel too. While they would appreciate formal contact with Israeli authorities, they get by on their own resources to remain abreast of relevant security threats and issues. These include open source intelligence, social media analysis, their own network of sources, and informal contacts with government officials. These informal contacts go deep in Israel, where the common bond of national service and employment within relevant specialised military, intelligence and law enforcement agencies help provide some level of contact between business and government.

Such firms provide an important information sharing link with others in the business community. They provide private policing, intelligence and protective security advice and support to their clients at a degree of intimacy that's generally unobtainable from government agencies.

Most of this support is about terrorism though. According to one interlocutor, serious and organised is the poor cousin of terrorism. Others contrasted the relative priority given to funding military forces compared to policing.

Interestingly, three interlocutors with extensive experience in financial crime thought that the media was the best way for business to understand the patterns of organised crime and its key protagonists.

It's all in the network

In summarising the Israeli approach to information sharing about crime, it's fair to say that the system relies upon *information transfers*, which are enhanced by

[31] Section 314 helps law enforcement identify, disrupt, and prevent terrorist acts and money laundering activities by encouraging further cooperation among law enforcement, regulators, and financial institutions to share information regarding those suspected of being involved in terrorism or money laundering (see https://www.fincen.gov/statutes_regs/patriot/index.html?r=1&id=314#314).

close personal and institutional contacts. In the case of financial crime, for instance, information flows from the institutions to government, and there is little formal feedback. Information sharing between the financial institutions is itself limited by law. Privacy concerns are paramount because 'everybody knows everybody' in Israel, which is promoted by a very active media.

Given those features, most of the interviewees for this project expressed their confidence in their personal networks. These allow an ongoing exchange of information in informal ways that suits the culture and priorities of the nation. It is hard to see how those without networks or the many small-medium enterprises can effectively participate in this system. Still, the system is described as suitable for this socio-political context.

Factors that promote information sharing about organised crime in Israel

- High levels of familiarity within society establish a reasonable basis for inter-organisational trust. Familiarity also creates deep and extensive personal networks.
- High threat environment, especially for terrorism (this may have some positive side-effects, but work on counter-terrorism is valued more highly than work on crime).
- Reporting regime about money laundering and (mandatory) terrorist financing, with a broad range of professions including lawyers and accountants (others including car dealers and precious jewelry dealers are marked next).
- Limited public debate about government's ability to gather and use information, within constraints of privacy laws.

Factors that inhibit information sharing about organised crime in Israel

- High levels of familiarity within society means privacy is a major concern where information sharing to counter crime is concerned (and Israel is described as a 'litigious society').
- INP has been described as 'still working itself out' and identifying the mechanisms it needs.
- High levels of immigration make it hard to vet non-Israel born people – this narrows the extent of networks.
- Corruption is a real concern, and Israel has experienced many nationally significant cases in the last decade.
- There's a view that the media will play an active and all-encompassing role in publicly identifying organised crime.

Annex B: United Kingdom

Context

The organised crime context for the United Kingdom is described in the *National Strategic Assessment for Organised Crime* by the National Crime Agency. This assessment identifies the key threats as including child sexual abuse, organised immigration crime, firearms (illicit importation and use), drugs, organised acquisitive crime, money laundering and economic crime. One component of economic crime is fraud, which costs the UK economy 'billions' of pounds per year. In addition, the UK terrorism threat is facilitated in some ways by links with organised crime and the current alert is Severe, meaning terrorist attack is highly likely. The impact of organised crime overseas is also noted as being inimical to UK interests, leading to extensive international cooperation. As a consequence, the UK faces a significant threat from serious and organised crime: cyber-crime is rated as a 'Tier 1' national security threat, while serious and organised crime is rated as a 'Tier 2' threat.[32]

While this leg of the research included discussions on counter-terrorism and organised crime in general, there was a specific focus on efforts to share information about fraud. This angle is particularly pertinent in the UK and London in particular due to the shared desire to make London a resilient and attractive place to do business.

Countering fraud, UK Style

Fraud is a particular type of economic crime that involves wrongful or criminal deception intended to result in financial or personal gain. Fraud can also deprive others of their rights and result in serious direct and indirect harms for businesses, government and society in general. In the latter, victims of fraud can experience serious mental and subsequent physical effects, as well as negative effects on their financial situation. Fraud also deprives governments of resources and requires significant law enforcement, regulatory and judicial resources to deter fraud, protect against it, and punish it. For businesses, fraud is a constant problem and significant frauds have bought some businesses down. In the main though, fraud adds costs to products directly as businesses add a margin to cover that activity, and indirectly as businesses need to invest in integrity systems and investigation capability.

In the UK, the anti-fraud system is comprised of a number of agencies who work within a particular legal framework for information sharing. A number of

[32] National Crime Agency, *Strategic Assessment of Serious Crime*, June 2015; HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, October 2010.

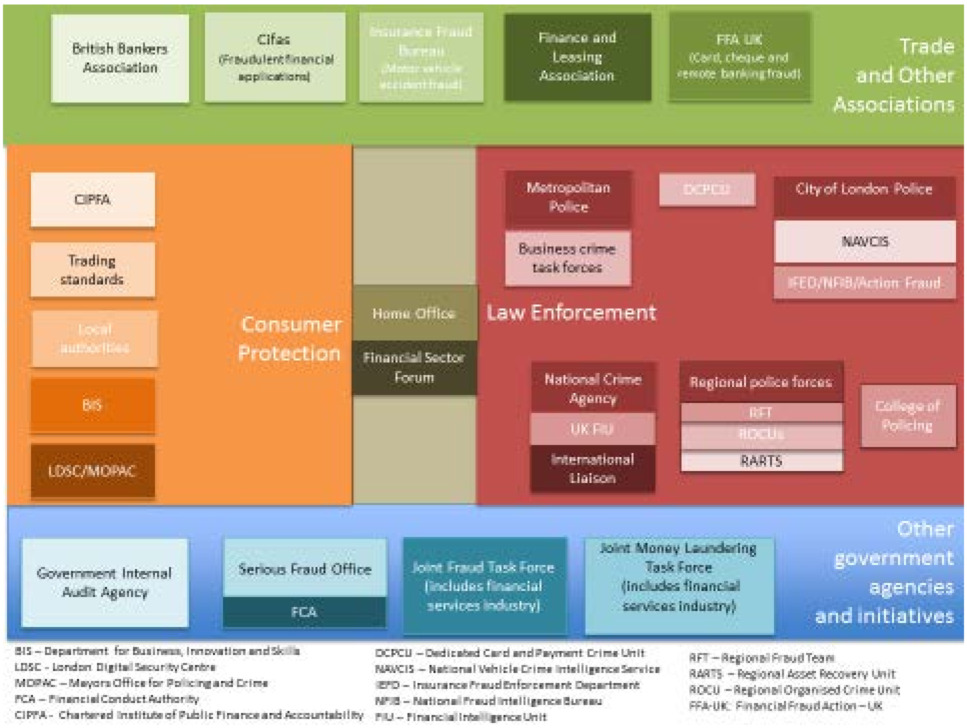
interesting innovations were encountered in the course of the research visit, and these are described below.

The anti-fraud landscape in the UK

The anti-fraud landscape in the UK is a great case study of information sharing about crime. This particular crime area—which is not the exclusive province of organised crime—features a number of industry-based information sharing groups, and arrangements to ensure compliance with legislation and provide focus on individual commercial concerns.

The anti-fraud landscape is sketched in Figure 3. This figure describes four key sectors, which are loosely linked through the Home Office. While the list of actors is relatively comprehensive, the diagram is unable to do justice to the actual linkages between them. A more complete representation would show linkages between some of the trade association bodies and the specialised police units; the cross sector membership of the joint task forces for money laundering and fraud; and the status of local government agencies (such as the Mayor's Office for Policing and Crime) and the local police forces. Indeed, this is a complicated environment that shows some elements of overlap, and perhaps some gaps.

Figure 3: The anti-fraud mosaic in the United Kingdom **(original source, Cifas)**


British Bankers Association
Cifas (Fraudulent financial applications)
Insurance Fraud Bureau (Motor vehicle accident fraud)
Finance and Leasing Association
FFA UK (Card, cheque and remote banking fraud)
Trade and Other Associations
CIPFA
Trading standards
Local authorities
BIS
LDSC/MOPAC
Consumer Protection
Home Office
Financial Sector Forum
Metropolitan Police
Business crime task forces
DCPCU
City of London Police
NAVCIS
IFED/NFIB/Action Fraud
Law Enforcement
National Crime Agency
UK FIU
International Liaison
Regional police forces
RFT
ROCUs
RARTS
College of Policing
Government Internal Audit Agency
Serious Fraud Office
FCA
Joint Fraud Task Force (includes financial services industry)
Joint Money Laundering Task Force (includes financial services industry)
Other government agencies and initiatives
BIS – Department for Business, Innovation and Skills
LDSC - London Digital Security Centre
MOPAC – Mayors Office for Policing and Crime
FCA – Financial Conduct Authority
CIPFA - Chartered Institute of Public Finance and Accountability
DCPCU – Dedicated Card and Payment Crime Unit
NAVCIS – National Vehicle Crime Intelligence Service
IEFD – Insurance Fraud Enforcement Department
NFIB – National Fraud Intelligence Bureau
FIU – Financial Intelligence Unit
RFT – Regional Fraud Team
RARTS – Regional Asset Recovery Unit
ROCU – Regional Organised Crime Unit
FFA-UK Financial Fraud Action – UK

The legislative framework

The primary focus for law about crime information sharing in the UK is the Data Protection Act (1998) – known as DPA. DPA is based around seven general principles, the most pertinent of which are: data is collected data only for specified purposes, kept only as long as necessary for that purpose, is processed fairly and lawfully, and is protected against unlawful use. There is a specific 'carve out' for national security, making this data exempt from the DPA, although other legislation applies. Section 29 also contains specific rights for tax and law enforcement agencies, generally allowing them to share personal information for their specific purposes and freeing them from their obligation to allow citizen access to held data. Importantly, the UK is trying to establish a culture where agencies 'dare to share' so they meet obligations or help other agencies conduct their respective functions.

There is no general exemption for law enforcement, and additional laws and codes of practice have been written to guide actual data sharing activities.[33] While a definitive statement of these laws is beyond the scope of this report, the key legislation and codes most cited by interviewees included:

- **UK Crime and Disorder Act (1998).** This act establishes an obligation for police and local councils to execute a strategy to reduce crime, disorder and drug use in their respective areas. This legislation requires the active cooperation of relevant organisations, and has led to specific protocols being instituted to allow information sharing.
- **Crime and Courts Act (2013).** This act establishes the National Crime Agency. Importantly, it provides the NCA with the power to receive information from anyone, and share information with anyone (Section 7).
- **Police Powers Act (1987).** This act provides law for compiling and sharing criminal records.
- **Home Office Code of Practice on the Sharing of Police Information (2005).** This code summarises the obligations for police in regards to information sharing. This codes states that 'chief officers may arrange for other persons or bodies within the UK or overseas to receive police information where the chief officer is satisfied that it is reasonable and lawful to do so'.[34]
- **Serious Crime Act 2007.** This act includes provisions to share information about fraud with anti-fraud organisations (section 68), offences for unauthorized disclosure of information (section 69), and an ability to conduct 'data matching exercises' which 'may not be used to identify patterns and trends in an individual's characteristics or behaviour which suggest nothing more than his potential to commit fraud

[33] See UK Data Protection Act (1998) at http://www.legislation.gov.uk/ukpga/1998/29/contents, especially sections 7 and 29. See also Information Commissioner's Office, 'Data Sharing Code of Practice', 2011; and advice on police information sharing from the College of Policing, available at: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/sharing/.

[34] Home Office Code of Practice on the Sharing of Police Information (2005), p. 12.

> in the future' (Schedule 7, 32A6). A code of practice for information sharing about fraud was also mandated (section 71).

Other legislation is consequential for information sharing too. For businesses, legislation places limits the information that competitors can share, although some data exchange that promotes competition is allowed.[35] Human rights, principles established in other professional fields (such as the 'Caldicott principles' in the medical field[36]), and common law also influences information sharing. Anti-money laundering regulations are also relevant because they can add duplication and so delay to fraud investigations.

Interviewees generally expressed the view that extensive information sharing about crime between government, business and the community was both possible in the UK, desirable and to some extent, occurring. Despite this, information sharing often needs to overcome practical barriers when attempts to do so are made.

Sharing information about fraud—the UK practice

The framework and legislation supporting information sharing about fraud in the UK seems to have promoted the movement of information between law enforcement and the trade and other associations for a significant period of time. Cifas and the two trade associations interviewed for this report—Financial Fraud Action UK (FFA UK) and Insurance Fraud Bureau (IFB)—all pointed to their own capabilities within their niche areas, which included an ability to present information in ways that police can use, and perceived their relationships with police as being strong.[37] They also explained how they can aggregate views and information, and then present that police information in an 'arm's length' way from individual businesses. For the two organisations associated with dedicated police units[38], the flow of information was seamless and constant.[39] However,

[35] OECD, 'Information exchanges between competitors under competition law', 2010, pp. 278-9 examines UK legislation and practices, especially the insurance industry exemption.

[36] These principles are: (1) Justify the purpose(s) of using confidential information; (2) Only use it when absolutely necessary; (3) Use the minimum that is required; (4) Access should be on a strict need-to-know basis; (5) Everyone must understand his or her responsibilities; and (6) Understand and comply with the law.

[37] Cifas is a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime (see www.cifas.org.uk). FFA UK is 'responsible for leading the collective fight against financial fraud on behalf of the UK payments industry' (www.financialfraudaction.org.uk); and IFB is 'a not-for-profit company established in 2006 to lead the insurance industry's collective fight against insurance fraud' (https://www.insurancefraudbureau.org).

[38] FFA UK is associated with the Dedicated Card and Payment Fraud Unit (http://www.financialfraudaction.org.uk/Police-The-dcpcu.asp). DCPCU is a partnership between the City of London Police, Metropolitan Police and FFA UK. IFB is associated with the Insurance Fraud Enforcement Department in the City of London Police (https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-

even these relationships were not without challenges that include a need for even more specialised training for these units.[40] Still, the success is such that the representatives interviewed did not question the value of both the trade association information groups and the dedicated police units.

New devices have been created to broaden the flow of information among government agencies, industry and the community (in a more limited way). One of this is a Joint Fraud Task Force that includes law enforcement, regulatory agencies, major financial industry representatives and organisations such as the trade associations and victim representatives. The aim is to better understand the threat, pass intelligence more easily, help victims of fraud, and harden the overall system. This group will also help implement a 'protect and prevent' strategy that aims to reduce fraud through better information and pertinent advice for businesses and the public. The NCA is playing a crucial role here, as their enabling legislation allows them be a pivot for the system.

The fraud landscape diagram above shows that many different actors have a role in countering fraud. In one sense, the sheer number of actors (and the desire to include more, such as victim representatives) represents a particular weakness in the information sharing system. Indeed, one of the aspects discussed in other examples was the way the time to establish such systems grows dramatically as more and different actors become involved.

Still, real benefits can be derived from diversity like this. Firstly, information from different sources can be obtained, which is useful for identifying an individual's patterns of behaviour. Further, analysis conducted in one sector might lead to the detection of fraud in another. The diverse powers of the different actors can also be used against a fraudster, including administrative sanction, criminal proceedings, and disruption by actions like closing accounts. And lastly, diversity can help to avoid 'capture' by a single interest group, which might either allow that group to leverage the partnership for other purposes, or result in system collapse if support is withdrawn. Since either would result in criticism of the network and the government, diversity has a broader utility than just the transactional value.

Cifas, FFA UK, IFB the DCPCU were all instigated well before the Global Financial Crisis of 2008, while the IFED was created in 2011. Despite their different timing, the two sponsored police units have assumed a particular importance in the periods of budget austerity. The direct funding from the trade associations has allowed police forces to maintain a relatively consistent level of resourcing for these crime areas, and indeed added additional resources to the overall crime

crime/ifed/Pages/About-IFED.aspx). Another police unit dealing with intellectual property (IP) crime is funded by the UK Government's Intellectual Property Office.

[39] This view was not universally held, and law enforcement agencies were still open to criticism that the flow of information was 'one way'. Interview with police official, London, March 2016.

[40] Discussion with police official, London March 2016.

effort. The relationship is not without risk however: perceptions of industry capture are often raised through this kind of work, and there is the real potential for public-private partnerships to sour very quickly if eithers' conduct is questioned. The British system of transparency (announcements and reports), steering committees that attend to governance and strategic priorities, clear respect for operational independence, and the use of trade associations (including Lloyds of London for the IFED) help to promote each organisation's integrity.

Yet, as one interviewee put it, it's no good sharing information if nothing is done. There needs to be a realistic expectation among those sharing information that some action will come of it. This need helps to explain why trade associations invest as they do. On top of that, a suitable level of skill is needed in the investigative force and judiciary, especially when it comes to newer forms of fraud. That interviewee was not confident that the latter was being widely satisfied in the UK, which meant a number of potential cases would not be followed to a conclusion.[41]

Information sharing to counter crime against business and the community

Implementing local counter-crime strategies

The UK Crime and Disorder Act 1998 introduced a requirement for local-level officials to develop a strategy for countering crime, disorder and drug abuse in their local areas (Section 6). This provision, in turn, opened an opportunity to share information with non-government partners as well.

Establishing the information sharing mechanism to enable these strategies was not straight-forward. According to Dr Spenser Chainey, an academic with direct experience in the emergent process, implementation of the legislation was not particularly vigorous at first. There was also significant uncertainty about what information could be shared, who could share it, and how it could be used. In his view, cultural resistance and not legislation was the main reason for the situation, and further education and process development was needed.

The situation began to improve after 2010. A report, 'National Support Framework', was developed and released to enhance understanding of the legislation and establish model process for the front-line implementers.[42] Creating agreed information sharing protocols, to which all parties acceded before joining the partnership, was a critical element. It created the trusted system and established both expectations of the parties and a way to sanction

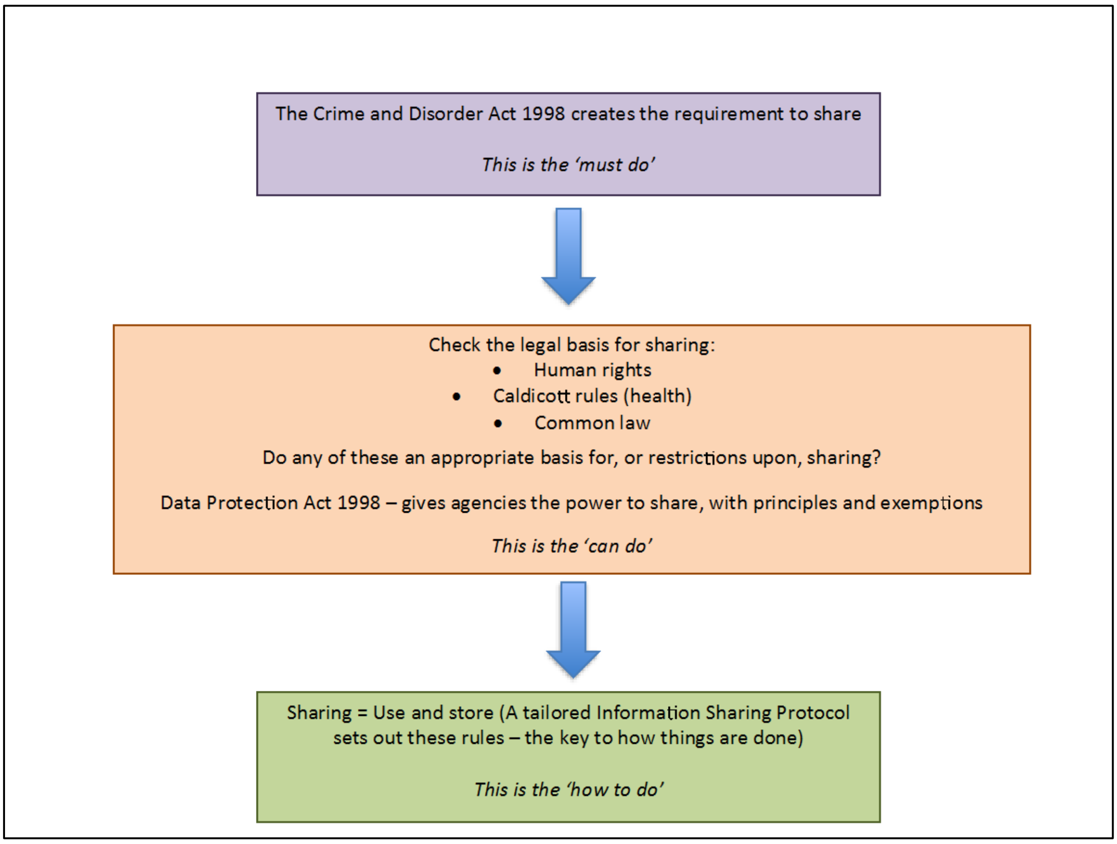
[41] Interview with police official, London March 2016.

[42] Home Office (UK), 'National Support Framework: Information sharing for community safety Guidance and practice advice', HM Government, London, 2010.

non-compliance. Dr Chainey found that enhancing confidence was also important, as officials were sometimes reticent to share even with trusted partners because they feared breaching the laws.

To assist this development, Dr Chainey developed a simple model (Figure 4) that explained the basis for sharing, and recommended small process changes to promote confidence in the participants. One of these involved an addition to the meeting 'sign-on sheet', which included a short reminder to all participants of their obligations under the information sharing protocol, and an affirmation that the participant understood those obligations.

Figure 4: The 'can do' model for information sharing in the UK context
(Source: Dr Spencer Chainey, University College London)


The Crime and Disorder Act 1998 creates the requirement to share
This is the 'must do'
Check the legal basis for sharing:
• Human rights
• Caldicott rules (health)
• Common law
Do any of these an appropriate basis for, or restrictions upon, sharing?
Data Protection Act 1998 – gives agencies the power to share, with principles and exemptions
This is the 'can do'
Sharing = Use and store (A tailored Information Sharing Protocol sets out these rules – the key to how things are done)
This is the 'how to do'

This example provides two main insights into information sharing in the law enforcement space. Firstly, permissive laws are necessary but insufficient. Since the legislative landscape is complicated and not always obviously consistent, effective implementation will rely upon education and clear guidelines for people who are at the action end of information sharing. This additional support will increase confidence among participants by helping them to understand how they can use the legislation to best effect. The second key insight is the need to constantly reinforce the information sharing protocols during implementation. While reinforcement may be as simple as the 'sign on sheet' remedy described earlier, it may need to extend to refresher training, informal activities and progress reviews to ensure the system remains understood and fit for purpose.

Programs to counter crimes against business

Crimes against businesses are a major concern for the Metropolitan Police ('The Met'), which is the force with responsibility for policing greater London. While mostly about 'volume crimes', the information gained by the Met from the arrangements described below can be relevant to localised aspects of organised and gang crime.

The Met have instituted a number of information sharing activities with business, and some specific parts of the community, to promote their aims. The focus point for their system is active cooperation with the Mayor's Office and local business, especially through a business crime reduction partnership with a local business peak body, 'Safer London'.

'Safer London' is an umbrella organisation to coordinate different crime reduction and sector-specific initiatives in the region. Membership of 'Safer London' is open to all businesses, with small- and micro-business being a particular target audience, and it is supported by the Mayor's Office and the region's major law enforcement agencies. Membership provides direct benefits to the business community including a secure wiki-site for information and intelligence sharing, access to radios and a communications network, and training and general information. Membership can also help relevant businesses demonstrate their obligation to improve the safety environment around their premises, which is a condition for some licences. The 'Safer London' umbrella is large indeed, for it covers sector-specific initiatives such as 'ShopWatch', 'PubWatch', 'Police and Security' and a 'Shared Radio Scheme'. Also covered is 'Project Griffin', which provides counter-terrorism awareness and training for London businesses.

The ways the Met itself organises its contact with businesses include:

- The Falcon Taskforce, which focuses on fraud and cybercrime. This taskforce responds to referrals from Action Fraud (see above).
- The London Digital Security Centre, which aims to secure and protect London's micro to medium size businesses against cyber risks and threats. This is a public-private partnership that provides threat intelligence, business services and community engagement,
- Operation Amberhill, which is a proactive information sharing activity focusing on false identity documents. This includes Operation Genesius, which is a partnership with the printing industry to reduce criminal access to the machinery and supplies needed to print false identity documents.
- Cross-sector Safety and Security Communications is established as a charity involving the public and private sectors. It aims to help businesses improve their safety, security and resilience through an information sharing hub that involves industry sector leads and official agencies.

- The Met are also considering creating an information fusion centre targeting organised crime. It's possible businesses could be linked into this centre, although it is too early to explain specifics yet.

The Met also incorporates civilian technology companies into their operations, and has seen a significant increase in private industry offering police-like services. One example is Face Watch[43], which offers retail store clients an integrated surveillance, intelligence and reporting system to counter theft and anti-social behaviour. The Met also encourages some 'critical friends' to discuss their programs and offer advice and perspectives. Charities are also engaged in some aspects to do with gang crime, such as the Safer London Foundation, which focuses on helping young people affected by violence and crime.

The Met's efforts to engage local businesses in crime prevention shows a number of sector-specific initiatives, some of which are linked to national initiatives. In most cases, these are ways for the police to pass information (including tailored messages and advice) to different constituent groups. Some feedback may be given to those who provide information, but that will mostly be in the form of verbal conversations and stakeholder meetings.

Forward leaning and risk accepting

Information sharing in the UK is conducted within a mature framework that includes over-arching legislation, different legislation and regulation for the law enforcement agencies, flexible structures and a certain level of trust. Most of the information shared is case-style information, although some organisations have the ability to share bulk data for research purposes.

The examples studied during this visit showed a high degree of collaboration (in terms of joint working and to-and-fro contact) between business and government in particular, and also some interesting ways of including the broader community and 'third sector' groups. This flexibility is often supported by task forces, which can be created relatively quickly and disbanded with little fuss to meet specific needs. Longer-term arrangements were also used, a number of which were described as now being very beneficial and effective. The ability of major London business associations to pay for additional services means that additional resources—including information and direct funding—are made available to law enforcement.

The UK system also appears to be risk accepting. The whole issue of private sponsorship for police is the most interesting example of this. While this method of creating additional police effort is used elsewhere (for example, at INTERPOL[44]), implementing this approach entails significant political risk and

[43] https://www.facewatch.co.uk/cms/

[44] INTERPOL has accepted direct sponsorship to conduct research and training in areas like sporting fraud, child sexual exploitation and cybercrime. This funding amounts to 29% of INTERPOL's budget (see http://www.interpol.int/About-INTERPOL/Funding/External-funding).

real reputational risk for all parties involved. In some areas like assistance to small business, low-level information is given to un-vetted business who can contribute to a shared local information picture. The risk of sensitive information compromise is low, but the ability to blame certain individuals for crime without due process seems ever-present.

The key issue about the future of information sharing in the UK relates to the people involved. Education about the permissions and methods available to share, and reinforcement of those, is an ongoing process, not a once-off. With such encouragement in place, and with the right safeguards, it is possible to conceive further initiatives or deeper engagement in time.

Factors that promote information sharing about organised crime in the UK

- Clear legislative and political support for information sharing that protects business.
- Business desire to protect themselves, which results a willingness to pay for additional 'intelligence' and police services.
- The ability to keep individual businesses at 'arms length' from law enforcement by way of trade and other associations, and the ability for the police (in particular) to maintain operational independence in their tasking.
- The NCA's information sharing mandate, and willingness of other police jurisdictions to engage business using a variety of methods.
- Good systems that are tried and tested.
- The use of government-led task forces that involve business and victim groups.

Factors that inhibit information sharing about organised crime in the UK

- Individual understanding of a somewhat complex legal framework.
- The somewhat complicated processes needed to create new arrangements.
- While a 'lag' indicator, the inability to follow through with all reported cases can make information sharing seem poor value in some instances.

Annex C: The Netherlands

Context

The Netherlands is a comparatively small European Union (EU) country that's also an important gateway to Europe as the location of Europe's largest port, Rotterdam. The country also hosts a number of international legal and crime institutions including the International Court of Justice and Europol.

The organised crime threat in the Netherlands consists of two overlapping networks. The first comprises transnational criminal gangs that use the roads, airport and especially the seaports to bring illicit goods into and out of Europe. Much of this crime transits the Netherlands and many of its perpetrators live outside the country or reside temporarily in the Netherlands.

Local groups are the second network. These groups live on the margins of Dutch society: generally family or ethnically based, and many in number. While these groups cooperate, there's no strict hierarchy or clan-based system that unites them. A number of these local groups participate in transnational activities within and outside Europe. For many however, their key markets are the nation's openly tolerant prostitution and marijuana scene, and the darker edges of both markets that include human trafficking, weapon smuggling and illegal narcotics. The Netherlands' main criminal exports are marijuana and synthetic drugs (it's also a transit country for other drugs), although fraud would be another one. Indeed, cybercrime including fraud is a key concern that attracts local and international enforcement attention in the Netherlands.

As a national security priority, organised crime is considered to be a 'second rung' issue in the Netherlands. More focus is placed on terrorism and, in a general sense, cyber threats. Individual crime concerns like human trafficking do get real attention, but this is often seen in the context of human rights. Attention on people smuggling and irregular immigration is also increasing.

It's also important to understand that the prime minister is relatively weak in the Dutch system, which means individual ministers are relatively independent of the centre. According to one analyst, this make collaboration across boundaries subject to the discretion of the ministers involved.

Law enforcement in the Netherlands is undergoing a massive restructuring, where the many provincial and local police forces are being incorporated within the National Police. The Ministry of Security and Justice also plays a national leadership role in policy, research and crime intelligence sharing.

Data and information sharing in the Netherlands is conducted under the overarching Personal Data Protection Act (1999).[45] This law implements EU directives and covers the familiar principles associated with contemporary data protection. However, it contains a number of exemptions from the law, including for security, intelligence and police purposes. The Police Data Act (Section 20) provides direct authority for the police to share information with other parties 'for the purpose of a collaborative arrangement of the police with persons or entities, in agreement with the competent authorities, to provide police data to such persons or entities, for the following and other purposes:

- the prevention and investigation of criminal offences;
- the enforcement of public order;
- the supervision of compliance with regulations.'[46]

Section 7 also contains provisions for protection of data (secrecy).

Other legislation can also be used to promote cooperative action among government agencies. The Public Administration (Probity Screening) Act, better known as 'BIBOB', has been a key tool in controlling the environment to screen-out organised crime. This Act allows local government to examine the history of an applicant for a permit in specified areas, including catering licenses, building permits, permits to dispose of waste and transport licenses for transport companies, housing corporations, cannabis coffee shops, brothels, gaming, real estate (when dealing with government), fireworks importation, boarding houses, and running smartshops, growshops and headshops.[47] Tenderers for specified work in construction, environmental, and information technology sectors also screened under BIBOB. This Act allows close information sharing about these matters within government, and it has been applied extensively to counter organised criminal activity at street level.

The Dutch attitude to government-business-public information sharing was described by one senior police officer as reflecting the 'welfare state' culture of the broader society. In the main, law enforcement is seen as a government function, and cooperation with business or the community consists mainly of

[45] Unofficial translation available at: https://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf accessed 24 March 2016.

[46] Extracted from 'Agreement on Collaboration and Information Exchange: Electronic Crimes Task Force (English Version)', Netherlands Police Agency, 2011, p.2.

[47] See Government of the Netherlands, 'Public Administration Act (Bibob) will be extended to intensify the fight against organized crime', February 2011, available: https://www.government.nl/latest/news/2011/02/21/public-administration-act-bibob-will-be-extended-to-intensify-the-fight-against-organized-crime, and 'New Public Administration Act effective as well as celebrating an anniversary, June 2013, available: https://www.government.nl/latest/news/2013/06/24/new-public-administration-act-effective-as-well-as-celebrating-an-anniversary . Among other products, 'smartshops' sell herbal products that are supposed to stimulate the mind, and 'growshops' and 'headshops' sell products to support cannabis production and consumption.

advice from police and information upwards from others. Little close collaboration was described in many areas, although one initiative in the electronic crime area is breaking that mould.

Dealing with organised crime – Amsterdam style

Dutch and Amsterdam authorities have applied an 'administrative approach' to countering organised crime in the famous 'red light district' (RLD).[48] This effort has involved two main projects: 'Emergo', led by the police and focused on reducing the ability of criminals to operate in the RLD; and '1012', a local government initiative to renew the city centre and place stricter boundaries around the drug and prostitution industries. The model is now being used in another Amsterdam location, Java Street. The relevant aspect of all this activity concerns how different government agencies came together to share information across their distinctive cultural boundaries and legal frameworks.

It took some time to establish firm information sharing agreements in the first two projects—and that was within government. Professor Cyrille Fijnaut, a participant and intellectual driver of the effort, recalled how negotiations involving police, local government and the tax office took over a year to be finalised. Others suggested the reason for that lay in the different perspectives and priorities among agencies. For example, an agency was not interested in a person unless that person was doing something wrong under the agency's legislation. Similarly, 'Amsterdam is a big city', and a resource-intensive focus on a small part of it might be hard to justify.

Obtaining political support for coordinated action was therefore a critical first step. That support was borne out of a major national scandal concerning undercover policing, which led the Dutch parliament to establish a commission under the leadership of the politician, Maarten van Traa.[49] The van Traa Commission, building on the theoretical work of the Fijnaut Research Group, began a series of activities designed to promote awareness of organised crime, identify syndicates, and develop further recommendations aimed at removing organised crime from the city.[50]

The different data sharing laws and agency attitudes towards data sharing were complicating factors in this effort, so these needed to be harmonized. BIBOB, described above, was implemented in 2003 as a way to apply administrative

[48] Cyrille Fijnaut, 'The innovative containment of organized crime problems in Amsterdam's inner-city, 1996-2015', n.d; Julie Ayling, 'Going Dutch? Comparing Approaches to Preventing Organised Crime in Australia and the Netherlands', Regnet Research Paper, Australian National University, Canberra, 2013; Edward R. Kleemans and Wim Huisman, 'Multi-agency approaches in "crimogenic" settings: the case of the Amsterdam Red Light District', *Crime, Law and Social Change*, 64:4-5, 2015.

[49] Edwin W. Kruisbergen, Deborah De Jong and Edward R. Kleemans, 'Undercover Policing: Assumptions and Empirical Evidence', *British Journal of Criminology*, 2010, pp.5-6.

[50] Fijnaut, n.d., pp. 3-6.

measures against organised crime. BIBOB helped information sharing in a limited but important way, because it compelled agencies to provide information to the operational arm of BIBOB within the Ministry of Security and Justice. This small group received access to tax, judicial, police and some data from the Chamber of Commerce, and were responsible for issuing 'BIBOB advice' (no risk, low risk or high risk). While only one input, this use of data—in a new context—constituted an important step forward in inter-agency cooperation.

But perhaps more important than compulsion was cultural change: the stakeholders themselves needed to become confident with each other and the mission. Professor Fijnaut described a culture that valued information protection and did not reward sharing. The police and tax agency, in particular, did not share information in the early days so BIBOB was only useful in stopping (some) serious criminals from exploiting the legal economy. Information sharing was also difficult because it involved asking more questions than usual. For instance, getting to know the real 'beneficial ownership' of a business was time-consuming and needed information from many departments. Developing a map of ownership for the complete RLD was impractical because it was both resource-intensive and unfocused. Efforts needed to be directed at the most important networks.

Focus was an important factor in this entire operation because prosecutors control investigations, not police: this places prosecution at the heart of the Dutch system. So there was a strong preference for working on actual cases rather than exploring trends and 'hypotheticals'.

What emerged from these negotiations and the Emergo experience was the model for the Regional Information and Expertise Centres (RIEC). The RIEC (which are based in the main regions and have a national headquarters in The Hague—which is called the LIEC), are a government-only group that analyses crime with relevance to their home region, and advises on legislative and administrative approaches to dealing with that crime. The development process involved close consultation with the Data Protection Authority, who provided advice on how to build the framework. Other work was done to ensure that RIEC information that would be subsequently used as evidence would satisfy criminal courts, and that the stakeholders (and information providers) would be satisfied with the processes. The network now has about 400 officers allocated.

The value of the LIEC/RIEC was shown in many ways. The national structure allowed learning from one region to be transferred to all. This meant knowledge about particular industries could be shared, such as unusual patterns of activities or dual uses for certain equipment. The existence of these organisations also freed resources to conduct research, which might be viewed as unwanted 'fishing operations' under the prosecutorial model and culture. The structure also created standards for information sharing that had been lacking, and the practical information technology solution needed to enable that cooperation.

Despite this, most people interviewed for this report think true collaboration with business and the community sector is rarely achieved. While civil society groups have some influence (for example, churches had an impact on human trafficking for a time), charities tend to take a low-profile role in this space. Most of the information about crime flows either as tips to police or advice from police. Information sharing between government and business might even be proscribed, as one interviewee remarked of the Tax Office under its legislation. Long-term collaboration cannot be assumed either. Even within government, the positive effects of project-based cooperation do not seem to survive long after the end of that project, according to Professor Edward Kleemans, a leading Dutch criminologist. On the positive side, elements of the administrative approach to dealing with organised crime can also be seen in another interesting innovation within government that focuses on counter-terrorism.

The CT-Infobox

While an internal to government arrangement, the Counter-Terrorism Information Box (CT Infobox) provides another example of how Dutch agencies collaborate.

CT Infobox was established as part of the Dutch General Intelligence and Security Service (AIVD) in 2004 and broadly (but not explicitly) authorised under the Intelligence and Security Services Act 2002 (Wiv 2002). It is, in effect, a multi-agency group that analyses information about possible terrorist cases and advices agencies to either (1) share information with another agency (which is likely advice for participating agencies to share information); (2) adopt a particular course of action with respect to a threat, or (3) initiate an operation. It is a 'closed box' so actual information about a suspect or threat does not get issued by the group, and agencies retain complete operational autonomy.

The box operates as a 10-agency grouping of experts that works within the AIVD. All are government employees with the highest levels of security clearance, and some (but not all) have a special status as Section 60 employees of the AIVD.[51] It is supervised by a coordinating board consisting of one representative of each participant, and headed (in 2015) by a police officer.

According to a recent review of CT Infobox, this group has been well designed for the task of information sharing. It makes good use of the 'dominance of the problem' by focusing on the critical issue of terrorism and violent radicalism in the Netherlands, while maintaining a partnership that does not compromise the

[51] 'Summary: CT Infobox 10 years', c. 2015, copy available from the author. Wiv 2002 identifies 'The commissioner of a police force, the commander of the Royal Netherlands Military Constabulary, the director-general of the national tax office of the Ministry of Finance perform activities for the General Intelligence and Security Service.' This means the status of other CT Infobox members, including the Prosecution Office, Department of Immigration, Social and Employment Department, Financial Intelligence Unit and the National Counterterrorism Coordination is ambiguous.

autonomy of the participating organisations. Its method of operation also addresses the key information security and privacy concerns of proportionality, limitation and subsidiarity since subjects discussed in the box are already suspected of terrorism (only) and no information leaves the box. In addition to an agency referral, individuals are assessed on referral to the Infobox by the participants to ensure they are likely threats, and are de-listed if and when they are no longer considered as threats. [52]

Multi-agency participation is a real strength of the Infobox. This grouping provides information to establish a '360 degree' view of a person, and to provide many ways to deal with a particular individual using the authorities and competencies of the participating agencies. The Infobox also allows agencies to de-conflict their activities in respect to individual cases.

The success of CT Infobox means some consideration is being given to expanding the type of information used in the box, such as by conducting strategic level analysis of the CT threat or by providing more resources so the box can undertake detailed analysis of individuals. There is some push towards giving it legal status under Wiv 2002. This latter move was considered important because management-level frictions arise at times because the legal basis for the arrangement was not absolutely clear, and as mentioned earlier, there is some ambiguity about the relationship of some box members to the AIVD. [53] The review also noted how it might also be used to counter organised crime as well—either through an extended remit or by the creation of a new 'Infobox'.

Operating the box comes with some challenges. IT connectivity was a problem initially and participants needed to return to their home agencies to gather requested information (this is improving). Small agencies can find it hard to sustain their involvement and the cost of participation can be unequal for them (and their concern might be magnified if activity against an individual does not engage their core responsibilities). Proving the value of the arrangement can also be difficult, but both the review and some familiar with its operations think the value measurement challenge is surmountable.

Despite these challenges, there is a high level of trust within the box and its value is accepted. While there are thoughts of changing it, the status quo is the most likely future for the CT Infobox. It is meeting a need, is not resource intensive (in a big-picture sense) and the participants are happy with the output. Major changes (expect, perhaps, legislative cover) might upset that balance at a crucial time.

While the two previous examples have highlighted successful intra-government collaboration, there is also promising business-government collaboration in the National Police's Electronic Crimes Task Force (ECTF).

[52] 'Summary', pp. 78-80.
[53] 'Summary', p. 81.

A new model of collaboration: ECTF

The years 2011 and 2012 saw a major spike in internet banking and payment fraud in the Netherlands. One response to this problem was the Electronic Crimes Task Force (ECTF), which is a true public-private information collaboration.

Formed in March 2011, the ECTF is a partnership between the National Police, the National Public Prosecutor's Office, and a number of financial institutions.[54] It is hosted within the National High Tech Crime Unit, a part of the Central Criminal Investigations Division. A supervisory committee sets the overall direction for the task force but does not interfere in operational decisions. This committee is chaired by a Deputy Police Commissioner and includes the National Cyber-Crimes Prosecutor, the Head of the High-Tech Crime Unit, representatives of all members (usually the head of anti-fraud and compliance) and a representative from the Ministry of Security and Justice. The committee meets every eight weeks.

All ECTF partners must sign a covenant, which sets out the role, legal basis, expectations and responsibilities of each member. The participants agree to bear all costs associated with their participation, assign at least one person full-time equivalent (FTE) to the ECTF, and agree to remain in the agreement for at least one year. There is an important air of 'equality' in the partnership, where every participant is expected to provide as much information as they can and be as responsive to requests as they can. These expectations are facilitated by the full-time presence of a skilled fraud investigator, with information links to their parent firm, within the task force office.

The actual office itself is a small room with 10 workstations. This intimate environment helps the group to facilitate its main functions involving intelligence, investigations and interventions.

Intelligence is case information in the form of responses to enquires about a particular customer, transaction or account. The information is only shared within the boundaries of the ECTF: what goes outside are 'suggestions' that the financial firms look closely at a particular customer or advice to prosecutors to start an investigation.

For the police, if there is sufficient reason they will recommend an investigation to the Prosecutor's Office who, as noted before, will decide upon the next steps.

[54] The full non-government membership list is: ABN-AMRO, Rabobank, ING, SNS Bank, the Dutch Bankers Association, and the International Cards Association.

The ECTF has undertaken a number of interventions, including one on money mules,[55] and another on money laundering via bitcoin.[56]

This system requires a high level of trust in both the operational model and the individual involved. The task force is able to short-cut the usual processes, which can take months, and to respond to emerging threats and methods. Indeed, the ECTF prides itself on looking for the new methods as it feels best place to identify and analyse these

When reflecting on the ECTF, a former senior member thought a dedicated investigative capacity and a liaison capability would help improve the operation. Measuring the value of the ECTF was also a challenge (as in many such organisations). There were significant opportunities too, particularly to grow participation and provide the police and prosecutors with more experience in cyber cases.

While this is a case of public-private partnership within the Netherlands, another public-private partnership among differ nations is also taking shape in The Hague at EUROPOL.

Multi-national and public-private: EC3

EUROPOL is the EU law enforcement agency. It's a collaborative policing activity that employs around 900 staff in The Hague to gather information about and track the most serious criminal and terrorist threats to the EU. Information gained at Europol is provided back to the individual national jurisdictions for arrest and prosecution.

The European Cybercrime Centre (EC3) began operations in 2013. It aims to strengthen the law enforcement approach to cybercrime by providing a central intelligence hub, investigatory expertise and source of strategic analysis. Its explicit desire to engage the business community in this effort makes it an interesting example of information sharing between these sectors.

EC3 grew from an existing meeting of national cybercrime investigation and intelligence leads, who collectively thought more could be done if their interaction was closer and more structured. The resulting group was formed with the expressed intention of bringing EU, international law enforcement and business groups into the same organisation to work of the most serious and challenging aspects of this crime type. To achieve this, EC3 developed an operational arm, which includes three focal areas and a multinational joint task

[55] DutchNews.nl, '200 questioned in Dutch-led crackdown on 'money mules', 1 March 2016, available: http://www.dutchnews.nl/news/archives/2016/03/european-police-target-money-mules-holding-e7-5m-in-bank-accounts/.

[56] Agencies, 'Ten arrested in Netherlands over bitcoin money-laundering allegations', *The Guardian*, 20 January 2016, available: http://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy.

force (JCAT). Its second arm conducts outreach, research, forensic analysis and strategic planning.

The business sector is engaged in EC3 in two ways. The first is through two advisory committees that help guide the strategic direction of EC3. The members of these committees, covering the financial sector and internet security sector respectively, are chosen from among applicants based on their professional expertise and ability to contribute to the group. The second method is to direct engagement of experts from major companies. These may be included on a case-by-case basis into the JCAT.

There are some legal complexities regarding this kind of information sharing arrangement, the most fundamental being the multi-national aspects. In the main, intra-EU information sharing about crime is covered under numerous regulations.[57] The ensure compliance, relevant information tends to be sourced through member countries, and analysis is passed back to member countries. This ensures compliance with relevant data protection regimes and reflects the practicality of EC3 mandate.

Might the situation change?

So far, the people interviewed for this project (with the exception of ECTF and EC3) have painted a picture whereby *information transfers* dominate the government-business-community triangle in the Netherlands. Given the two more recent innovations around financial and cybercrime, it's entirely possible that this situation could change in the direction of greater *information collaboration* in time.

The cause of that change is likely to lay in both public pressure and a greater enthusiasm for cross-sector collaboration. A number of interviewees explained the demands from local communities and businesses to have more engagement in setting priorities, and a greater willingness to pay for additional policing resources. The latter was being observed at local levels, where 'neighbourhood watch' style committees were becoming better organised. Real-time information was also in demand, spurred by the capabilities of web technologies and social media. This latter capability had the effect of 'making myself the police's number one priority', according to a senior policeman.

The demand for the type of information was also broadening. Businesses in particular wanted information about criminal techniques and persons (not just events), and to understand weak spots in forensics and investigative techniques. There was not a high demand for 'strategic' information at the local level, but businesses do want advance notice of new criminal techniques and targets so

[57] For an overview of these regulations and arrangements, see EU Migration and Home Affairs, 'Information exchange', available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/information-exchange/index_en, accessed 24 March 2016.

they can adapt in time. Still, the overwhelming demand was for information about what to do now in response to a criminal threat.

If success does breed success, then collaborative efforts like ECTF, RIEC/LIEC and CT Infobox might provide relevant models. Still, better information sharing about organised crime will not come for free. It would pose additional costs upon government and business, and might also require new legislation to ensure information sharing is on a sound basis.

Factors that promote information sharing about organised crime in the Netherlands

- Mandated sharing through BIBOB.
- A dedicated research and advisory organisation in the RIEC/LIEC and Dutch Ministry of Security and Justice.
- A number of successful intra-government models including Emergo and CT Infobox.
- The close integration of academic research with counter-organised crime activities.
- Shared threat perceptions, especially in the counter-fraud area.
- Close cooperation with the Data Protection Authority.

Factors that inhibit information sharing about organised crime in the Netherlands

- 'Welfare state' approach that sees countering crime as government's responsibility.
- Limited view of what the community sector could provide, but note close relationship with academia (but a lack of think-tank attention).
- Government focus on countering terrorism tends to crowd-out threat from organised crime, especially where it is perceived as mainly 'transnational'.

Annex D: The United States

Context

'Organised crime' was first given this label in the United States, initially to brand the secretive mafia groups that perpetrated large-scale criminal activities.[58] From there, the organised crime threat to the US has expanded in every conceivable way, and is now considered 'a significant and growing threat to national and international security, with dire implications for public safety, public health, democratic institutions, and economic stability across the globe.'[59] While the US focus on organised crime is nation-wide, priorities can differ from region-to-region. For instance, mafia-style crime, financial crime and terrorism are the major concerns in New York, while industrial espionage and cybercrime attract significant attention in San Francisco. Drugs are a common concern, although the views around marijuana enforcement vary considerably across the country.

The multidimensional nature of the organised crime threat is reflected in American law enforcement arrangements. The complexity of this system is well documented: with over 17,000 police jurisdictions, any number of agencies will have a role to play in countering organised crime in general, or investigating a particular case. There are also a number of interagency task forces, information fusion centres and coordination centres that deal with organized crime in broad or narrow ways, reflecting the challenges of coordination and information sharing across these jurisdictions.[60]

Information sharing about crime is simultaneously constrained and liberal in the US. Constitutional guarantees of liberty, together with a level of opposition to 'big government', mean information sharing initiatives are closely watched by the courts and civil society groups. At the same time, the level of threat to the US from both criminal and terrorist activity, and the exponential increase in the amount and variety of data held by firms and government, creates a strong imperative to share and the means to do so. Today's context for this activity is strongly influenced by the 'Snowden release' of thousands of US government documents that detailed the intelligence gathering activities of the US and other governments. This breach has had many effects on information sharing, including a reported perception that businesses want to know more about threats to them because they think the government has more information than they admit to.

[58] The first recorded use was in Chicago in 1919 – see K. von 'The Concept of Organized Crime in Historical Perspective', 1999, available: http://www.organized-crime.de/lauhtm01.htm.
[59] National Security Council, 'Transnational Organized Crime: A Growing Threat to National and International Security', available: https://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat. All links provided in this report were live on 16 April 2016.
[60] Carter 2015, p. 525.

The legal framework for information sharing about crime is diverse and voluminous, and so difficult to simplify. In relation to terrorism, these include the 2002 USA PATRIOT Act, 2002 Homeland Security Act, and Foreign Intelligence and Surveillance Act (as amended in 2008). For organised crime, enabling law includes Criminal Intelligence Systems Operating Policies federal regulation (28 Code of Federal Regulations [CFR] Part 23).[61]

Presidential Executive Orders, which also have the status of law, influence information sharing and privacy policy. An example of the former is the 'Executive Order—Promoting Private Sector Cybersecurity Information Sharing', which authorizes the information sharing and analysis organisations on a firmer footing (see later discussion).[62] These orders allow the government to act in a unified way, and are made public through the Federal Register.[63] Another example, 'Empowering Local Partners to Prevent Violent Extremism' recognises the need for broad collaboration that involves the community, and recognises the need to focus engagement on more than just national security while leveraging existing relationships based on areas such as health, education and civil rights.[64]

Presidential policy directives also play a role in enabling information sharing, and can do so at the classified level. In particular, recent presidents have developed information sharing strategies[65], and provided policy guidance on areas such as cybercrime, cybersecurity, transnational crime and privacy. The latter has come into focus since the major data breach at the Office of Budget and Management in 2015, and the response has included a new Presidential Privacy Council. Another recent order has established a presidential council on privacy, which aims to establish an 'interagency support structure' to provide skills development and advice on privacy matters.[66]

A national strategy to counter transnational organized crime was launched in 2011, and has building 'new partnerships—with industry, finance, academia, civil society and non-governmental organizations—to combat transnational

[61] 28 CFR Part 23 applies to the Regional Information Sharing Systems (see https://www.riss.net/Default/Overview).

[62] President Barak Obama, 'Executive Order—Promoting Private Sector Cybersecurity Information Sharing, 13 February 2015, available: https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[63] Randolph D. Moss (acting Assistant Attorney General), 'Legal Effectiveness of Presidential Directive, as Compared to an Executive Order', 29 January 2000, available: http://fas.org/irp/offdocs/predirective.html.

[64] President Barak Obama, 'Empowering Local Partners to Prevent Violent Extremism', August 2011, p. 5, available: https://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.

[65] President Barak Obama, 'National Strategy for Information Sharing and Safeguarding', December 2012, available: https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf.

[66] President Barak Obama, 'Executive Order—Establishment of the Federal Privacy Council', 9 February 2016, available: https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.

crime networks that operate in the illicit and licit worlds' information sharing as one of its five policy objectives priorities.[67] This same strategy recognises that not all of our capabilities have kept pace with the expansion of 21st century transnational criminal threats', while accompanying commentary said countering organised crime received a lower priority than terrorism in the period after 9/11.[68]

Accompanying the increased priority to countering organised crime is the significant amount of attention that is being given to sharing information about cybersecurity. As President Obama reinforced in his 2015 State of the Union address, the national effort in the cyber domain is continually being modified and expanded. Most recently, this has included the Cybersecurity Information Sharing Act 2015, which provides a mechanism for sharing case-based cyber threat indicators and defensive measures automatically between participant government and non-government entities.[69] This initiative will rely upon close cooperation and the realisation of mutual interests between business and government.[70]

But as the research for this report was underway, a major disagreement between Apple and the Federal Bureau of Investigation was playing out. While not about information sharing *per se*, the differences in priorities between some elements of business and governments (among others) were plain to see. Also clear was just how great the challenge of information sharing between the sectors is going to be, as the differences are about culture as much as legislative, structural, physical or scale issues. Needless to say, there have been a number of attempts to promote closer relations, and a number of different models are on display in the US. Some of the longer-running initiatives are in the field of critical infrastructure protection, where both the Federal Bureau of Investigation (FBI) and, more recently, the Department of Homeland Security (DHS) play leading roles.

The FBI and information sharing

The FBI runs four main public-private information sharing activities with increasingly smaller groupings. The pinnacle, which involves major companies, is the Director's own Domestic Security Alliance Council (which focus on criminal acts against interstate commerce); next is the Strategic Partnerships Program, which has a counter-intelligence focus; and the broad base is InfraGard, which

[67] President Barak Obama, 'Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security', 2011, p. 14, available: https://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[68] 'Strategy to Combat Transnational Organized Crime', President's covering letter.

[69] Department of Homeland Security, 'Privacy Impact Assessment for the Automated Indicator Sharing (AIS)', DHS/NPPD/PIA-029(a), 16 March 2016.

[70] Tami Abdollah 'U.S. Homeland Security department to share cyber threat data', *Canadian Underwriter*, 18 March 2016, available: http://www.canadianunderwriter.ca/insurance/u-s-homeland-security-department-to-share-cyber-threat-data-1004082255/.

shares information to protect critical infrastructure. Additional programs include the Cyber Initiative Resource Fusion Unit, which is co-located with the National Cyber-Forensics and Training Alliance. This report will focus on the last DSAC and InfraGard, while noting that a re-think about information sharing is underway within the FBI.

InfraGard

InfraGard is a national, FBI-lead association that promotes information sharing between government and the operators of critical infrastructure. Its first chapter was opened in 1996 and focused on cyber security. The remit expanded after the 2001 terrorist attacks to include physical attacks and a broader focus on cyber and other crime types.[71] InfraGard is now associated with the Department of Homeland Security as well, and covers sixteen critical infrastructure sectors. The overall scheme is managed by a national leadership body, and comprises over 80 chapters with over 55,000 members across the US.

The stated purpose of InfraGard is to share information and intelligence to prevent hostile acts against the US. This sharing usually takes the form of presentations, meetings, conferences, an electronic noticeboard, and a helpdesk managed by the Louisiana State University on behalf of the FBI.

Each chapter is run slightly different, but all are established as 501(c)(3) not-for-profit organisations. Each chapter has a board that guides its activities in close cooperation with the local FBI field office. Membership of InfraGard is open to a US citizen who has an interest in a critical infrastructure sector. This includes state and local police, company representatives, academics, and practically any individual who cares to apply. Each applicant undergoes an FBI criminal history check, but actual membership is granted by a chapter's board. The actual membership list is not released by the FBI and is closely protected. While membership is therefore vetted, meetings are typically open to the public.

The operations of InfraGard chapters are managed on a volunteer basis, although some employ coordinators to manage their chapter's affairs. The FBI also assigns a point of contact who attends board meetings and represents the FBI, but the level of additional official support will differ from chapter to chapter.

The FBI funds the national-level support infrastructure, but members agree to bear their own costs for participation. Local chapters may levy dues on their members, or charge to attend presentations and conferences. Some chapters attract corporate supporters. Any money raised by a chapter remains with the chapter.

InfraGard's mandate for information sharing is relatively limited, and views of its effectiveness are mixed. The meetings and presentations are high-quality but

[71] FBI, 'InfraGard: A partnership that works', 2010, available: https://www.fbi.gov/news/stories/2010/march/infragard_030810.

unclassified affairs, but only a very small proportion of the members actually attend these. Content for the electronic noticeboard is controlled by the FBI, and members are not permitted to post to it. According to one interviewee, who is an active member, these factors limited InfraGard's ability to be a true information exchange.

Two other interviewees remarked how InfraGard was not a really 'trusted' network because the membership base was too wide. While all members have undergone police checks, not all are considered to be experts in their field so other professional networks were more important as facilitators of sensitive or technical information exchange than InfraGard. This last point is especially relevant to the earlier discussion about the ability of trusted systems to create interpersonal trust among members who do not otherwise know each other.

InfraGard has also been criticised from the outside. A 2004 paper published by the American Civil Liberties Union claimed InfraGard was 'turning private sector corporations – some of which may be in a position to observe the activities of millions of individual customers – into surrogate eyes and ears for the FBI.'[72] A 2002 media article also criticised InfraGard for providing its members with information that was not available to the general public, and even political leaders. That same report also criticised InfraGard's media management policies.[73] InfraGard is also described as 'secretive' and 'powerful', with an expanding scope that helps the FBI's investigative mission into all types of crime. Given the scope of the information available to InfraGard's private sector members, one critic asks whether 'is it possible that InfraGard will be a domestic police and spying arm for the government concerning "thought crime"?'[74] While much of this criticism can be contextualized in the American debate over the power of government and its relationship with business—not to mention wide of the mark—these points should be considered in the design of any information sharing arrangement with limited membership.

Domestic Security Alliance Council

The Domestic Security Alliance Council (DSAC) is an FBI and DHS-led initiative to share information about crime and security as it affects major US businesses. DSAC was established in 2005, and formally chartered in 2012. DSAC is led from the FBI Director's office, and has a board consisting of over thirty member companies.

[72] Jay Stanley, 'The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society', American Civil Liberties Union, 2004, p. 12.

[73] Reporters Committee for Freedom of the Press, '"InfraGard" lets FBI disclose sensitive information to select few', 2002, available: http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-winter-2002/infragard-lets-fbi-disclose#sthash.rIiKReLs.dpuf.

[74] Gary D. Barnett, 'InfraGard: An unhealthy Government Alliance', available: http://fff.org/explore-freedom/article/infragard-unhealthy-government-alliance/

DSAC aims to provide a venue and means for senior law enforcement and security officials to exchange information and advice with major US companies. There are currently around 360 members and these are large, 'Fortune 500' and 'Fortune 1000' enterprises. Each member is vetted, and they receive access to relevant tailored intelligence through a secure portal. DSAC also conducts training activities for corporate chief security officers.

The DSAC wants to operate in a style that allows members and government to 'collaborate, resolve problems, exchange best practices, and share intelligence and information with one another'.[75] DSAC also helps headquarters divisions and field offices coordinate their activities with these companies, and build networks among the participants.

Most DSAC information is behind the secure portal, but some general information is released publically through the website.

A rethink is underway

The FBI is also rethinking their approach to partnerships. An interviewee explained that the current arrangements were costly to sustain, and the success of each is difficult to measure. The current arrangements also mean that businesses often need to deal with more than one FBI contact. Critical audiences were also not being reached, especially in the small and medium enterprises, while the flow of information was predominantly outwards from the FBI and collaborative opportunities were not being maximized. There is also a need to build greater trust with industry, particularly those in the high-tech sector who tend to be culturally indisposed to cooperation with law enforcement.

Information Sharing and Analysis Centres (ISACs)

The ISAC system informs and helps private sector industries in 'critical infrastructure' domains to protect themselves against cyber and physical attack. First established in the financial sector in the 1990s as a response to the emerging Y2K cyber threat, and have since broadened their focus to include protection against physical attack after 9/11. There are now 21 ISACs recognised by the National Council of ISACs in the US.

While initially established by the critical infrastructure sectors in response to a Presidential request and later formalised through Presidential Decision Directive 63, 1998 (and updated by later Presidential Policy Directives), ISACs are private industry groups. ISACs facilitate information sharing and analysing threats to the individual sectors, as well as across the critical infrastructure sectors and with government through public-private collaboration.

[75] Domestic Security Alliance Council, 'Member Benefits', available: https://www.dsac.gov/about/dsac-member-benefits.

The public-private collaboration is coordinated through the Department of Homeland Security, and its role is outlined in the National Infrastructure Protection Plan[76]. This plan outlines the structure for public-private collaboration, including national-level councils for government and industry, 'sector specific agencies' that lead governmental efforts, intra-government (all levels) coordination mechanisms, regional public-private partnerships, academic centres of excellence and research, and the individual ISACs themselves.

The four generic roles for an ISAC are:

- **Centre of Expertise:** ISACs are a source of expertise for industry and government to access relevant, timely and actionable information from owner/operators and associations within a particular sector or sub-sector.
- **Representative Body:** ISACs represent the owners and operators of critical infrastructure. They collectively present the sector perspective versus an individual enterprise perspective and they protect organizations within the ISAC from attribution.
- **Information Centre:** ISACs provide a trusted hub where timely, actionable and relevant information is gathered from sources such as government, vendors, other ISACs and members of the respective sectors. This information is further analysed for relevance and potential impact, and shared amongst the stakeholders. Information shared centers around threats, vulnerabilities, incidents, best practices and mitigation strategies. Sharing can occur a variety of ways including via a listserver with attribution, over a secure portal, which can foster security, pushed alerts and through machine to machine sharing referred to as security automation. This information is shared under a non-disclosure agreement, and individual messages are marked using a traffic light protocol to denote sensitivity and dissemination protocols. ISACs also undertake other related activities like exercises, education and training.
- **Affinity Group:** ISACs act as a venue for collaborative efforts within a particular critical infrastructure sector, across the sectors and with government during times of threat and incident response. They work together to foster situational awareness and coordinate response activities. [77]

ISAC are established as either 501(c)(3) or 501(c)(6) not for profit organisations. Many have a governance structure which consists of an elected board representing the member organisations. While the funding method for each ISAC can be different, most are funded through member subscriptions. These subscriptions vary across the different ISACs, and are aimed to meet a level that

[76] Department of Homeland Security, 'NIPP 2013: Partnering for Critical Infrastructure Security and Resilience', available: https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf.

[77] Healthcare and Public Health Sector Coordinating Council, 'Comprehensive Charter' (Version 1.5), p 6, available: https://www.dhs.gov/sites/default/files/publications/Healthcare-SCC-Charter-2014-508.pdf.

will attract members across the sector. These members usually are owners/operators within their respective sectors and vetting each member is important for building the trusted community. Since only organisations can be members, vetting for most is relatively straight-forward because the organisations are well known.

ISACs share timely, relevant, actionable all-hazard (both cyber and physical) information around threats, vulnerabilities and incidents as well as best practices and mitigation strategies. In the cyber field, that information usually includes meta-data called indicators of compromise (IOC) such as IP addresses, subject lines in emails, malicious attachments, exploits and vulnerabilities which allow members to understand a potential threat, weigh against enterprise risk and then follow an appropriate course of action. This results in one organization's defense becoming the community's offense.

A number of lessons about information sharing were discussed in interviews for this project. Firstly, trust, value and infrastructure play a key role in fostering information sharing by ISAC members. When sharing moved from anonymous to attributed sharing, the sharing escalated. This was because members were able to see who was sharing, see the value in the information being shared and then clearly understand how the information could be shared further via the TLP. They were able to build relationships through the sharing mechanism and this created the community of trust.

Secondly, ISACs must continually demonstrate value for the participants. As with any organisation, when there is a subscription fee to participate, the member must realise value from the relationship in order to keep engaging and paying subscription fees. The growth amongst the ISAC memberships and in the number of ISACs themselves (now at 21), demonstrates a measure of success. Government agencies will also need to see value in participation, and one commentator has questioned the commitment of DHS to the ISAC system (but not some other agencies).[78]

Educating the sectors about the ISACs and the value of these communities as well as encouraging new membership is a third challenge. Providing information to the whole sector is the aim of each ISAC, especially those with interdependencies between large and small-medium enterprises. Constantly building reach into the sectors creates efficiencies for sharing, alerting, collaborating and coordinating response. Making enterprises aware of these initiatives, benefits industry, governments and countries and serves to protect as well as keep critical infrastructure resilient.

[78] Robert B. Dix Jr, 'Blog: Situational Awareness Will Inform Risk Management Decision Making', 5 May 2016, available: http://www.afcea.org/content/?q=Blog-situational-awareness-will-inform-risk-management-decision-making#sthash.9m7Gx84T.dpuf.

National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA) is a public-private partnership specialising in countering cyber threats through information sharing amongst and across industry and government within a trusted environment. Founded in 2002, the NCFTA is focused on identifying, mitigating, and neutralizing cyber threats globally through three main programs:

- The Cyber Financial Program (CyFin) is dedicated to the identification, mitigation, and neutralization of cyber threats to the financial services industry.
- The Brand & Consumer Protection Program (BCP) focuses on the fraudulent utilisation of the Internet for the sale of retail goods, including fraud related to e-commerce transactions as well as the physical distribution of counterfeit merchandise.
- The Malware & Cyber Threats Program (MCT) is dedicated to researching, identifying, and providing timely alerts through data feeds and proactive intelligence on cyber threats under analysis.

The NCFTA operates as a 501 (c) (3) nonprofit corporation with a board of directors drawn from the telecommunications, technology, consulting, legal, accounting services, and financial industries, as well as higher education. It has a complement of approximately 100 people, about half of whom work for the NCFTA, with the remaining team members coming from US and foreign law enforcement agencies and various industries. The NCFTA also has an extensive network of affiliates and member organisations in the US and overseas.

The NCFTA operates by conducting real-time information sharing and analysis with subject matter experts (SME) in the public, private, and academic sectors. Through these partnerships, the NCFTA identifies cyber threats in order to help partners take preventive measures to mitigate those threats. Participants in The NCFTA must sign a confidential membership agreement to participate, and the alliance has strict non-disclosure requirements.

Their information sharing activities are case-based. For instance, partners may make requests of each other to find a name, find more information and identify the target's activities. This kind of information is used to track threats. NCTFA staff might also analyse a cyber threat to identify how to combat it, and pass the information to members. The NCFTA does not conduct bulk data mining.

The NCFTA uses communications platforms such as listservs, working groups, and peer calls to discuss which issues are being seen in various industries and how best to address them. Once a majority of stakeholders agree that a given issue should be prioritised, analysts are tasked with research and analysis, with the aim of producing 'actionable intelligence'. This intelligence may simply take the form of feedback or an announcement, but it might also be used to develop cases or assist investigations. No classified information is held or produced.

The NCFTA also utilises its Internet Fraud Alert (IFA) system to report stolen account credentials discovered online.

New York Police Department

The City of New York Police Department (NYPD) has a significant and long-standing focus on information sharing with business and the community. The main focus of sharing examined for this report relates to counter-terrorism, which is a critical concern in the city. This is not the sole NYPD focus of course: it manages a number of information sharing initiatives to promote crime prevention, emergency management, and investigations.

Many initiatives were in place before 9/11, including the NYC Police Foundation[79], a charitable body that supports police capacity and capability development, and the 'APPL' program of business liaison that morphed into NYPD Shield after the devastating terrorist attacks of 2001. Shield is the NYPD's main focus for private sector counter-terrorism engagement, but not the only mechanism.

Counterterrorism Division and NYPD Shield

The NYPD's response to terrorism and engagement with corporations and local businesses is conducted through a number of programs based in the Counterterrorism Division and Intelligence Bureau. These programs support the part of the NYPD's counterterrorism strategy that seeks to isolate terrorists from the business support they may need, so they can better detect plots and protect the city.[80]

The Counterterrorism Division's NYPD Shield program is the Department's 'public-private sector partnership' that provides a central point of contact for information sharing with businesses about counterterrorism, acts as a conduit for business concerns about counterterrorism to the city government, and provides an 'umbrella' for other current and future programs. Launched in 2005, the NYPD Shield program now has over 16,000 members.

NYPD Shield provides services including advice on threat warnings, best practices, lessons learned, training courses and assistance with exercises. It can approach businesses on either a geographic or industry basis. Advice is provided through patrol borough counter-terrorism officers, regular member meetings to maintain links outside crisis periods, and quarterly conferences. NYPD Shield also distributes intelligence analysis products to its members, and uses the email list for day-to-day information about transportation, security and safety in the city, as well as for information about special events. It also provides similar services to other public agencies.

[79] The New York City Police Foundation was established in the 1970s, to 'provide critical resources for innovative NYPD programs that make New York a safer place to live, visit and work'. See www.nypolicefoundation.org.
[80] Discussion with senior NYPD officer, 22 March 2016.

Future initiatives are likely to occur outside New York, as NYPD aims to help other cities create their own 'Shield' programs.

NYPD Shield works closely with other areas of the Counterterrorism Division, including the 'Threat Reduction and Infrastructure Protection Section' (TRIPS). TRIPS is responsible for identifying critical infrastructure in New York City. The Section also promotes contact between NYPD and operators of critical city infrastructure or iconic places. The contact includes regular meetings and other contact with the operators, security planning for important infrastructure and events, and inspections and recommendations to maximise a facility's protection from terrorist attack. The squad also maintains contact with other Federal Agencies including Homeland Security, State, Secret Service and Transport; and state and local agencies such as the Department of City Planning and the Ports Authority. While their recommendations cannot be enforced, TRIPS advice is considered when building permit applications are decided by the City.

Operation Nexus is a complementary initiative run by the Intelligence Bureau, where business owners are encouraged to report suspicious customer transactions that may relate to terrorism. Upon a successful application as a Nexus partner, NYPD officers work with the business owners to help them understand terrorist methods and needs, and how this may interact with their business. Intelligence Bureau also manages the NYPD 1-888-NYC-SAFE line, which is a dedicated line for counterterrorism tips by the public.

The success or otherwise of Shield is hard to judge. Metrics like membership, numbers of civilians trained, downloads/views and product output help understand the penetration of Shield initiatives. These do not speak to preparedness, but the NYPD is confident that the system represents the best available under the conditions and that the Program is a "force multiplier" in the fight against terrorism.

Lower Manhattan Security Initiative

The Lower Manhattan area encompasses a number of iconic sites such as Wall Street and the new World Trade Centre complex. The desire to enhance security in this area saw the NYPD, NYPD Foundation and a number of major businesses develop a new information-sharing partnership in 2005.

The aim of the Lower Manhattan Security Initiative (LMSI) is to improve security in the 1.7 square mile area of the island. There are 41 partners in the LMSI, all of who are vetted and required to sign a memorandum of understanding concerning data sharing. Compliance with that memoranda is audited by NYPD.

The focus of the LMSI is a command centre based around the Domain Awareness System. This system integrates data from many systems: active CCTV, chemical detection sensors, and automatic facial and license plate detection. There is a 'shot spotter' capability, and access to geospatial data like building blueprints. Companies in the area also contribute information from their own cameras (which are the vast majority of the total), and security managers and guards.

Different users have different levels of rights in the system, and information can be filtered down to different geographic areas to increase the relevance of information to participants. Mobile capability is being developed as well, so that patrol officers and business can have access to data as needed. This capability will provide 'correlation workboards' to patrol officers, which provides them with information about people, locations and past events at or near given addresses.

Information within the command centre is shared on both bulk data (inwards) and case based (inwards and outwards). The outward flow is assisted by daily briefings and incident-specific advice. At present, 19 of the participants place liaison officers in the LMSI command centre.

One factor assisting this cooperation has been the recruitment of former law enforcement officers into companies. This recruitment, which was also remarked upon by a senior officer from a non-NYPD agency, also helps build the informal network of information sharing.

Real-time Crime Centre

The Real-Time Crime Centre—also sponsored by the NY Police Foundation—is a data analysis and research centre that provides intimate information support to the City's detectives. What is most interesting for this study is the way commercial information providers play a vital role in the centre. One company provides a portal that interrogates hundreds of federal, state and other governmental data bases to provide information such as addresses, asset ownership and aspects of a person's financial history. Criminal history and other judicial information can be accessed through the Federal Department of Justice.

NYPD Crimestoppers

The Crimestoppers program in NY is run by a cell within the NYPD. Its basic purpose is to provide a way for members of the community to provide information anonymously, and provide cash rewards where the information is used to make arrests. While the unit is part of the NYPD Detective Bureau, the reward money is provided by the NYPD Foundation. This creates an arm's length relationship between the taxpayer and those who receive the rewards.

Support like no other

NYPD operates in a very constrained space, with a very large force and generous 'off budget' financial support from its foundation. This level of resourcing places NYPD in a most unusual situation and allows it to manage a range of information relationships. That said, information collaborations with the business community is possible, especially through the NYPD Shield program and the LMSI. Both programs are described as having very deep roots in the business sector, and these programs provide ample opportunities to exchange information about terrorist and criminal threats.

New York City Emergency Management (NYCEM)

NYCEM is a city government-run organisation. Its relevant focus for this study concerns the way it provides information and advice to businesses and the community throughout the crisis life cycle.

Given the number of potential constituents for NYCEM, the system functions through 25 ‘umbrella organisations’, rather than directly to each individual business. These organisations have a seat in the emergency management operations room, and are responsible for the passage of relevant information to their stakeholders. NYCEM also uses monthly meetings, emails and webinars to keep in contact with the umbrella organisations. While most of the information traffic is ‘outwards’, there are open lines of communications upwards to NYC, including through those monthly meetings. The type of information being shared is ‘public’, case-based information.

NYCEM works closely with NYPD, especially where cyber incidents affect the city’s infrastructure. In times of emergency, NYCEM provides a liaison officer to the NYPD operations centre.

Social media and web-based platforms

Conversations with law enforcement about information sharing with the broader community usually started and ended on the topic of social media. While not a particular focus of this study, the use of social media for information sharing in law enforcement is growing in importance in a number ways. This growth is being driven by new platforms, and because this way of communicating has benefits for two-way communication and investigations.

In addition to general and global social media platforms like Facebook and Twitter, there are number of more specialised platforms operating in the US. One particular type of platform (of which there are a few different varieties) aims to give residents a better understanding of events in their neighbourhood. Platforms such as these allow members to sign on to a specific and small geographic area (often much smaller than a suburb or city ‘neighbourhood’ and sometimes within a few blocks around their residence). These platforms provide news feeds from mainstream media, information from police and city councils, and posts from their neighbours. Information is received via daily update emails or in real time on the website. These are free services.

One such service is ‘Everyblock’ (www.everyblock.com) operates in a number of major US cities. This service is provided by media corporation Comcast, and started as a way for local media organisations to remain abreast of events. It was also used as a way of providing local content to users at a time when news outlets were being amalgamated into larger units.

In today’s format, Everyblock has also become a platform for police ‘Open 311’ information (non-emergency requests for assistance), council notices like road closures and building permits, and events like neighbourhood meetings and block parties.

Everyblock is managed as a business unit of Comcast. Most control is maintained locally by Comcast local media outlets, who maintain a moderating function on the bulletin board. The company is able to monitor direct uptake and use very accurately, as well as identify where its content is used by others.

The next steps of Everyblock include finding ways to link communities without geographic definition, integrating further data and displaying it graphically or geo-located, and making hyper-local discovery easier. There is also the challenge of remaining ahead of the competition, as platforms such as www.nixle.com and www.nextdoor.com.

Nixle is especially relevant to local police-work. Its platform allows users to select police and local government information sources and receive alerts and regular update emails as desired. The original Nixle is aimed at the community, and a 'business version' is being developed at present. Its parent company, Everbridge, is an information integrator and communication service provider for emergency management and law enforcement.

New smart phone applications are also being developed to allow the public to report crime. These include an application available to New York State residents that allows them to take a photo of a crime or something suspicious, and have it uploaded to the police.[81] Residents of Chicago can use a similar application, and provides a central point for police to disseminate information including mugshots of wanted persons and the location of registered sex offenders nearby.[82] This type of application is drawing upon the vast data repositories in the US and 'open government' initiatives, which of themselves create other opportunities for information sharing about crime.

Bulk data

The Economist newspaper recently observed that 'online crusading and organising'—i.e. human communication—'will turn out to matter less to politics in the digital age than harnessing those ever-growing piles of data.'[83] That does not make case information irrelevant to the future, but it certainly places a spotlight on the increasing relevance of bulk data sharing and big data analysis to information sharing.

Like other jurisdictions, bulk data sharing is difficult in the US due to privacy concerns. That doesn't mean that bulk data is unavailable or not used. Indeed,

[81] See iHLS, 'Reporting Crime With Your Smartphone', 2 December 2015, available: http://i-hls.com/2015/12/reporting-crime-with-your-smartphone/.

[82] iHLS, 'Civic Apps: Can They Help Fight Crime?' September 2014, available: http://i-hls.com/2014/09/civic-apps-can-help-fight-crime/.

[83] Ludwig Siegele, 'The signal and the noise', *The Economist*, 26 March 2016, Special Report, p. 4.

the US tech giants such as Google, Facebook, Apple and LinkedIn (to name a few) hold significant amounts of information about the digital lives of American citizens, and they are looking to ways to monetize that freely-given data.[84]

This means the 'shared triangle of interest' actually shares a great deal of data already. That data comes largely from individual citizens who leave 'digital exhaust' as they conduct their lives through the internet. Massive quantities of data are also captured as citizens interact with their government. Much of that data is also provided online by 'open government' data initiatives that were originally established to help citizens keep their governments accountable. As Eitan Hersh, an academic, points out, that intended use is being inverted as political parties use data to identify voter preferences, propensity to vote and ability to donate—and rebuff attempts to make less data available for those purposes.[85]

There is a tremendous amount of data about individual US citizens on the internet, and a number of firms that specialise in collating that data or being an interface with repositories. These firms are used by law enforcement agencies as convenient, broad and deep repositories of data that will help, once analysed, to provide information and intelligence for operations and investigations.

One such provider is Lexis Nexis and their database service, Accurant. Accurant draws upon data held by Lexis Nexis and in open source repositories to provide detailed descriptions of individuals.

Another more publically-available service is 'Instant Checkmate' (www.instantcheckmate.com'). This service allows subscribers who undertake not to misuse the information (e.g. for credit history checks, to stalk or to take any other detrimental action) to search for criminal histories, phone number ownership, social media profiles and associates. The service also tracks registered sexual offenders who may live near or have connections to a particular person.

It's important to note that the data provided by Lexis Nexis and Instant Checkmate is still case information: questions are asked about individuals (or their characteristics) are answered individually.

Strong, contrasting pressures on information sharing

There are a large number of ways that information can be shared between government, business and the community in the US. While the balance of that activity falls at the *information transfer* end of the spectrum, some highly collaborative mechanisms have emerged too. As in the other nations studied,

[84] For analysis (amid advertising), see Accenture, 'Creating revenue from customer data', available: https://www.accenture.com/hk-en/insight-data-monetization-summary.aspx.

[85] Eitian Hersch, *Hacking the Electorate*, Cambridge University Press, 2015, cited in Siegele, p. 8.

case information dominates the type of information shared the in the US organisations studied here.

Information sharing in the US faces sharp internal and external critiques from the left and the right. The left critique of the surveillance state has been accentuated in the post-Snowden environment, while the perception that only the large corporations can participate in effective information sharing is also prevalent. This critique sees sharing as available only to the large companies, and not small and medium enterprises. From the right, distrust of big government also extends to some areas of business, while others can be concerned about the cost of information sharing upon their bottom line. Some also think that government knows far more than they disclose when sharing information, which can create difficulties. There's also an internal critique about effectiveness and cost, although strong political and leadership support also exists for information sharing.

What overcomes these contradictory concerns is the shared interest in maintaining a strong, prosperous and secure society. This has led to a number of different mechanisms being established over the last two decades—perhaps too many. Still, this brief survey of the United States shows that secure information channels that allow knowledgeable people to exchange information are valued. There is an increasing focus on real-time information sharing, particularly in the cyber domain, and this is encouraging new arrangements that may have broader applicability in time. Close collaboration is dependent upon a deep respect among the parties, particularly where the independence of agency judgment is concerned.

Factors that promote information sharing

- In the terrorism, cybersecurity and critical infrastructure sphere, a strong sense of national priority.
- Clear political will to include business in national security.
- Innovative partnerships, especially where private enterprise and government share costs.
- Charitable giving to promote information sharing solutions.

Factors that inhibit information sharing

- Cultural mistrust of big government.
- A certain level of dismissiveness of the effectiveness of large, membership based information sharing mechanisms to promote collaboration.
- Judging the return on investment.
- Security culture, especially where 'national security' information is relevant to law enforcement situations.

Annex E: Meetings

Note: Interviewee names have been removed for publication

Israel

Sector	Organisation: position/function
Industry	Security: CEO
Industry	Security: Consultant
Industry	Security/Intelligence: Consultant
Industry	Bank: Head of compliance
Community – academia	Independent criminologist
Government – law enforcement/regulator	Israel Money Laundering and Terror Financing Prohibition Authority (IMPA) – Legal
Community – academia	Interdisciplinary Centre Herzliya: Academic
Community – academia	Interdisciplinary Centre Herzliya: Academic
Community – academia	Interdisciplinary Centre Herzliya Academic
Government – police	Israel National Police: Financial Crime
Government – law enforcement policy	Ministry of Justice Senior official
Government – other	Australian Embassy Diplomat
Community - academia	Ministry of Public Security: Analyst
Community - academia	Ministry of Foreign Affairs: Counter-terrorism
Community – academia	Prime Minister's Office: Counter-terrorism
Government – other	Ministry of Foreign Affairs: Regional director
Community – academia	Ministry of Foreign Affairs: Counter-terrorism
Government – law enforcement policy	Ministry of Foreign Affairs: Cyber Security
Community – academic	Interdisciplinary Centre Herzliya: Academic

Community – think tank	Israel Democracy Institute: Analyst

United Kingdom

Sector	Organisation: position/function
Industry	Regulated products: Illicit markets investigators
Government – police	Australian Federal Police: Regional Manager, Senior Liaison Officer
Community – academia	City of London Police: Senior Officers
Government – police	National Counter Terrorism Policing HQ: Senior officer
Government – police	Metropolitan Police: Senior Officers
Community – academia	University College London: Research Associate
Government – other	Information Commissioner’s Office: Senior Officers
Industry	Trade association fraud control (1) Managing Director
Industry	Trade association fraud control (2) Managing Director, Director of information
Community – association	Private association fraud control Senior officers
Government – police	Economic crime police unit Senior officers
Government – law enforcement	National Crime Agency Senior Officers
Community – association	London Digital Security Centre – Senior executive

Netherlands

Sector	Organisation: position/function
Government – police	National Police Regional Criminal Investigation Division: Senior officers
Government – police	Regional Unit Amsterdam – National Police: Chief Constable
Government – law enforcement policy	Ministry of Security and Justice: Head of Strategy, Innovation and Research
Government – police	Electronic Crimes Task Force: Former head and fraud analyst

Government – law enforcement	Regional Information and Expertise Centre – Amsterdam: Program Manager
Community – academia	Criminologist
Community – academia	Criminologist
Government – law enforcement	National Information and Expertise Centre: Senior officer
Government – law enforcement policy	Ministry of Security and Justice: Organised Crime Research Centre
Community – think tank	Hague Security Delta: Deputy Director
Community – think tank	Stichting Toekomstbeeld der Techniek (STT): Senior Analyst
Government – police	Regional Unit Oost – National Police: Police Chief
Government – police	Europol – Electronic Cyber Crime Centre: Head of Business and Head of Strategy
Government – police	Europol: Australian Liaison
Community – think tank	Hague Centre for Security Studies: Executive Director and Analysts
Government – other	Australian Embassy, The Hague
Community - academia	Centre for Service Robotics: Researcher (fraud)

United States

Sector	Organisation: position/function
Government – police	New York Police Department (NYPD) International Liaison
Government – police	Counter-terrorism: NY Shield Program
Government – police	NYPD Counter-terrorism: Business Security risk assessment
Industry	Illicit market investigator
Community – nonprofit	National Cyber-Forensics and Training Alliance
Government – police	NYPD Operations Centre
Government – police	NYPD Crimestoppers
Government – police	NYPD Lower Manhattan Security Initiative
Government – police	NYPD Real-Time Crime Centre

Government – police	NYPD Facial Recognition Technology Unit
Government – law enforcement	NY-NJ Ports Authority Precinct Commander
Industry	Comcast – Everyblock
Government – police	San Francisco Police Department – senior officer
Government – police	Oakland Police Department – senior officer
Government – other	Information Sharing and Analysis Centre – senior executive
Government – law enforcement	Federal Bureau of Investigation – crime departments
Government – law enforcement	Federal Bureau of Investigation – public-private partnerships
Government – Law enforcement	Federal Bureau of Investigation - Cybercrime
Industry	High Tech Crime Investigators Association
Industry-Government	Presidential Innovation Fellows
Industry	InfraGard
Industry	Lexis Nexis