Project Morpheus:

Examining the potential to utilise Data Harmonisation to enhance international organised crime policing capabilities

Project Morpheus:
Examining the potential to utilise Data Harmonisation to enhance international organised crime policing capabilities

An Oxon Advisory ‘Emerging Technologies and Strategies for Public Safety’ Series Report

www.oxonadvisory.com

Please note: The views expressed in this research represent those of the anonymised individuals who spoke to the research team and not any of the researchers or any organisations affiliated with them or the project

BUCKINGHAMSHIRE NEW UNIVERSITY
EST. 1891

OXFORD BALTIC CONSULTANCY GROUP OÜ

Oxon Advisory

CRIMINIS
Training and consultancy services

Researchers

Dr Chris Allen - Buckinghamshire New University and,
Tony Lock - Oxford Baltic Consultancy Group OŮ

Researcher Bios

Dr Chris Allen is a researcher, lecturer, consultant and commentator specialising in organised crime and how it operates. He has significant experience in lecturing on cybercrime, drug trafficking, human trafficking, money laundering and firearms trafficking, among other subjects.

He is a Senior Police Practice Tutor at Buckinghamshire New University, where he is responsible for managing the evidence-based research projects Police Constable Degree Apprenticeship students complete in Year 3.

Concurrently, he is a Director of Criminis Training and Consultancy services, which provides a range of training courses to law enforcement, universities, and the private sector. He is also a specialist trainer with the Police Science Dr Academy and the London Policing College, he leads the *Policing Insight* coverage of organised crime and is a member of the Global Initiative Against Transnational Organised Crime Network of Experts and an Associate of Oxon Advisory.

Tony Lock works as an organised crime consultant, in the field and in academia, researching the intersection of crime, technology and harm. He has presented multiple papers in the UK and internationally. He is currently researching the State Actor and Organised Crime Nexus in the Baltic States and completing a book '*Working Undercover*, the Praxis of Covert Investigation' to be published later in the year. He is MA (Oxon) (1992) and holds an MBA in Information Technology and Management from Bayes Business School and has a Certificate in Knowledge of Policing.

Synopsis

In Greek Mythology, Morpheus is the God of dreams. Given that when pursued to its fullest extent Data Harmonisation (DH) and the idea that all law enforcement information could be pooled and all knowledge shared in the fight against crime is the ultimate dream, the name seemed appropriate for this blue sky thinking piece of research, which will examine the potential for DH to enhance existing operational, tactical and strategic capability in the long term.

While the project is named after the God of dreams, its aims and objectives are based firmly in reality. Recently CEPOL hosted a conference entitled *Preparing Law Enforcement for the Digital Age* (CEPOL 2022), this report will build on that theme and ensure policing is fully aware of the potential of new technology and the opportunities and challenges this brings when considering the development of new intelligence databases and the merging of existing ones. Specifically, through a mixed method approach the report will test the validity of the concept of merging databases to gain operational, tactical and strategic benefits as a viable future path for policing.

The research has been conducted in 'ideal world' sandbox scenario to allow participants to think freely regardless of current budget constraints in their own organisations or jurisdictions.

In practice this means the research won't be framed in the climate of the economic downturn as the piece is focused on actions that could benefit the public in the long term and therefore would not be subject to funding restrictions relating to the current climate.

Specifically, the report will look at 'what is being done' 'what can we do' and then finally 'what should we do' and what the challenges are around doing it. It is hoped this report will act as a feasibility study, offer an unbiased (as much as any research can be unbiased) and rigorously researched body of work that examines the benefits and challenges of a DH approach and what that should mean for the policing of organised crime groups that span borders much like multinational corporations.

The funding for this piece of work came mainly from the Buckinghamshire New University (BNU) Policy Support Fund with contributions from Oxford Baltic Consultancy and Criminis Training and Consultancy Services. The funding enabled fieldwork (semi structured interviews) to take place in Skopje - North Macedonia, Washington DC - United States of America, Bogota – Colombia, and Tirana - Albania. The locations were chosen as they are either strategic hubs for law enforcement or organised crime (or both). In total approximately 35 semi-structured interviews were conducted.

Introduction

Before the deep dive, some definitional clarity: According to the University of Michigan (2022) Data Harmonisation (DH) is defined as “all efforts to combine data from different sources and provide users with a comparable view of data”.

Definitions of what constitutes organised crime vary widely from country to country. Organised networks are typically involved in many different types of criminal activity spanning several countries. These activities may include (NCA 2019) trafficking in humans, illicit goods, weapons and drugs, armed robbery, counterfeiting and money laundering. Since the year 2000, the United Nations Convention against Transnational Organized Crime (2000) has provided an internationally shared definition of an organised criminal group as “a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit.”

While The National Crime Agency (2018) defines an OCG as “Individuals, normally working with others, with the intent and capability to commit serious crime on a continuing basis, which includes elements of planning, control, coordination, structure and group decision-making”; it also adds a caveat that this definition does not require the OCG to have committed serious crime only the intent to do so.

However, Europol (SOCTA 2017:13) say this definition does not adequately describe the nature of modern organised crime networks arguing that “OCGs operate in a criminal economy dictated by the laws of supply and demand and are favoured by social tolerance for certain types of crimes”.

According to Interpol (2018:2). “Organised crime is transforming. Traditional structures headed by powerful kingpins controlling niche crimes are increasingly replaced by loose, flexible criminal networks that shift operations and modify their business models based on opportunities, incentives, profitability and demand.”

The global nature of organised crime is one of the few areas that all sections of academia and policing can take a consistent view on (Allen 2023). The fact that there is no singular definition of such a vital concept does not bode well for a DH approach that would need to span multiple jurisdictions.

The Home Office, in its serious and organised crime strategy (2018:6) gives the clearest public indication yet of the sheer scale of the threat posed by organised crime, stating that in terms of deaths and impact on citizens organised crime is “the most significant national security threat the UK currently faces.” They conservatively estimate (caveating that much of it is hidden so the true cost is likely higher) that it costs the UK £37 billion annually.

Wainwright (2016) argues that drug cartels have learnt “brand franchising from McDonalds, supply chain management from Walmart and diversification from Coca-Cola” In short, internationalisation has made OCGs more sophisticated over the last 40 years (Allen 2023). As the seminal UNODC Transnational Organised Crime Threat Assessment (TOCTA) (2010) noted, groups in the top-scoring 20% of those mapped are predominantly involved in violence, money laundering, and drugs. Moreover, 79% of OCGs are linked to at least one quasi-legitimate business enterprise, which complicates the investigative perspective, but also offers a whole range of open-source data possibilities.

It's not just the international element of this problem that is challenging, organised crime also has a local element. Research by the Police Foundation and Perpetuity Research (2017:8) on the impact of organised crime in local communities, argues that organised crime is constantly changing and that while traditional activities such as drug dealing and serious acquisitive crime feature prominently, they are now commonly “supplemented with ‘new’ or emerging’ crimes”. They suggest a “more proactive, problem-oriented approach and a shift towards identifying and tackling the hidden dimension of organised crime”.

Given the internationality of organised crime, this can be aided through a more through grasp of trends at a national and international level through an enhanced DH approach.

The following report will collate and assess the ideas and insights of key practitioners as to how data harmonisation may supply ‘progressive thinking’ in tackling the key threats and harms of transnational organised crime in the medium and longer term.

Law enforcement capabilities

Regional Organised Crime Units (ROCUs)

In the UK, nationally, there are several examples of databases where information is shared such as The Police National Computer (PNC) and the Police National Database (PND), as well as Organised Crime Group Mapping (OCGM), which gives a summary of OCGs activities. However, forces also retain their own databases, which often have much greater detail than those submitted to national systems.

Current approaches vary significantly depending on the organisation and the level at which it is involved in policing. Both wider anecdotal evidence and interviews conducted for this project suggest locally forces are often wary of sharing data between themselves, while regionally the His Majesties Inspectorate of Constabulary and Fire and Rescue Service (HMICFRS) Regional Organised Crime Unit (ROCU) inspection in 2021 criticised the piecemeal and varied nature of cooperation, which is in part down to the temporary nature of their funding. *HMICFRS (2021)* note most UK forces have force intelligence bureaux (FIBs) as their intelligence hubs with spoke systems of varying complexity to coordinate intelligence collection and to deliver intelligence products to the front line.

Traditionally, forces have created 'confidential' units to firewall the transmission of sensitive intelligence between forces and agencies. However, Recently, a Sensitive Intelligence Network (SIN) has emerged in the UK (HMICFRS 2021). The SIN is made up of 18 law enforcement agencies, including the NCA and the nine ROCUs. Each ROCU serve between three and seven constituent forces. Their primary functions are to provide a range of specialist capabilities to forces and to lead the regional response to serious and organised crime. These include covert operations, surveillance, undercover policing, confidential unit, regional asset recovery team, cyber, operational security, government agency intelligence network, prison intelligence and SOC operations.

HMICFRS further noted since they were introduced ROCUs have evolved and have grown considerably in both the level of their resources and the type of specialist work they undertake. They found that ROCUs had good access to intelligence and performed well, despite dealing with many disparate IT systems they also found 'some excellent work led by committed people working in a complex and difficult environment... but too many examples of inconsistency in approaches to governance, IT and evaluation'

"The additional core capabilities now include asset confiscation and enforcement teams, undercover online, Government Agency Intelligence Network disruptions, regional organised crime threat assessment, dark web investigation teams, digital investigations and intelligence, child sexual abuse and exploitation, human trafficking, modern slavery, serious violence and county lines. As a result, ROCUs are far bigger organisations now than they were when they were first established**.** The ROCUs we visited all had a sensitive intelligence unit and varying levels of operational capability to investigate and disrupt OCGs that operate across police force boundaries."

It is clear from the above that the UK already has a sophisticated ability to share restricted information between various elements of law enforcement, the problem comes when you get down to the less sensitive pieces of information shared at a force-to-force level, which are just as vital to building a case against an OCG.

A former detective superintendent with ROCU experience notes that 'PND [the Police National Database] is not match fit' and added that they "don't see anywhere a huge appetite to take that problem on. We will need, unfortunately, another tragic death for that to be worked out".

"If you had asked me 10, 15 years ago, how were we were [at sharing information], I would have said we're quite good. But unfortunately, things have slipped back because technology has moved on, our ability to store data and retrieve data has moved on, the number of entities and databases we've got that contain risk has moved on. Our ability to automate and interrogate and share that data hasn't moved on at the same pace."

He also spoke about the political dimension involved in large scale projects "From a technical perspective, this is going to take more than five years to identify and solve. And therefore, nobody wants to take it on because it's too big".

"I paid somebody, as an external contractor, three years ago, to write a ROCU IT strategy. And they basically started off by saying, 'This is the scope of everything that's wrong currently within your ROCU network and this is technically where you should be looking forward. And then actually, if you want to commit to a strategy, you need to find the money' and policing basically went, 'that's too f****** complicated.

"My position would be we're really crap in the UK at sharing with anybody in policing. And we have to drag people to the table to share. There are rich, rich datasets available in surveillance control rooms, from surveillance logs. There's rich data in comms data, that's not shared anywhere. Phone downloads are not going anywhere. Banking details, proceeds of crime investigations. All that data that is often sat in a silo or on a folder somewhere, on an online folder in a police force's server room, and we don't do anything with it.

"As an East Midlands ROCU representative, you're going to have to have five icons on your desktop that take you into the five different forces. And you have to log into each one, into their separate databases to be able to research and interrogate them, which is neither ideal nor efficient really.

One officer, a cybercrime specialist currently serving in the National Crime Agency, noted the legal challenges of sharing information between different sections of policing and how crossing an international border with the data complicates things further

“I suppose if you look at the UK structure in terms of information sharing with 43 forces, done in 43 f****** completely different ways and everybody having a different opinion, and you needing everybody’s agreement to do it, that is then multiplied by f****** about 10,000 times with the EU alone, without including Interpol within there as well.

“GDPR has complicated it to such a level that law enforcement agencies are tied in knots, and I mean daily, with data sharing agreements, not just with private and commercial partners, but with other public-sector organisations. It is bonkers, to be honest”.

National Crime Agency

HMICFRS also inspected the National Crime Agency (NCA) in 2020 (HMICFRS 2020), the UK’s premier body dedicated to tackling organised crime and found that the NCA should improve the way it receives, collates and assesses intelligence and how it shares intelligence within and beyond its organisation. It also noted access to the Police National Database (PND) isn’t readily available to the staff who need it.

Positively, the inspectorate found improvements in the NCA ability to process and analyse bulk data, and investment in mobile digital devices that help staff securely communicate more effectively. It noted that the NCA should continue to invest in technology if it wishes to keep pace with the growth in bulk data. For example, technology able to better assess intelligence generated from the new ways in which organised criminals communicate.

On a similar vein, sources within the organisation indicate the NCA is developing a ‘dare to share’ policy to widen its range of intelligence sharing (both internally and externally) from ‘need to know’. As part of the change programme, it will set the right balance between ‘need to know’ and ‘dare to share’ which will improve the intelligence that it collects and will reduce the risk of intelligence not being shared appropriately. This will be similar to the processes used in counter-terrorism policing, and will result in changes to structures, policy and training. This is a cultural shift for many in the NCA, especially those who have always preferred to keep intelligence sharing to a minimum.

Dare to Share is a key component of any DH strategy and it is imperative that the reality matches the commitments in the press release if tangible improvements are to be made

One interviewee with current national organised crime policing experience, notes the challenges of having responsibilities split between the police and NCA.

“The danger is the agency go down one route; policing goes down the other route and we can’t share documents. Rather than driving between police stations with memory sticks we’ll be driving between agencies and police stations with memory sticks.

“We are the masters at working in silos and against each other at ‘x’ amount of wastage pounds to the public taxpayer.

He goes on to talk about how on a live operation when covert assets are being deployed the amount of information shared is a personal decision by the Senior Investigating Officer.

“If you deploy an undercover officer into an organised crime group you probably wouldn’t want that widened out. my partner in Counter Terrorism or my opposite number in ‘x’ region, would I be happy with them knowing. I probably would. Would I be comfortable that the Neighbourhood Inspector was aware of a covert operation? No, I wouldn’t.”

Police ICT as a whole

As a well as a reluctance to share information between services there are also challenges around the technical capacity to do so. In 2019, the police governance advisory CoPaCC released its ICT in focus report (CoPaCC 2019), which took an in depth look at effectiveness of this area and found that far from being able to make large sweeping innovative changes, police officers and staff are experiencing a range of minor issues that are impeding effectiveness

“Officers who need more than 20 different passwords and log-ons to access the various systems to do their job, to those waiting weeks for basic printer repairs, users being issued with new hardware and software that is already out of date and potentially unfit for purpose, training that’s delivered two years before systems are implemented or lasts less than 10 minutes, and operating systems that are so old manufacturers no longer provide support”.

Another issue CoPaCC found, similar to that identified by HMICFRS, was consistency between the level of service that forces received. User satisfaction with IT varied from 61% of Wiltshire to 6% for Staffordshire. Phrases such as “archaic”, “unreliable”, “unfit for purpose”, “not user friendly” and “painfully slow” appeared regularly in relation to both hardware and software (CoPaCC 2019:6).

The call for a more joined up and harmonised approach to data sharing is not a new one, and the 43-force structure- with the amount of independence it gifts each chief constable- is certainly not the ideal vehicle for it. This point is echoed by several interviewees from the CoPaCC Report. One neighbourhood officer stated: “The NHS, RAF, ARMY, and RAC all work nationally, and we should without doubt work nationally on IT. We should all work on the same crime reporting, dispatch and intel IT infrastructure at the very least” (CoPaCC 2019:6)

CoPaCC (2019) also notes that several forces were involved in collaboration projects at different levels, including Hampshire and Thames Valley Police, who operate a joint ICT department, and North Wales, who were part of a tri-force Niche project alongside Merseyside and Cheshire [Niche is a records management system (RMS) used by law enforcement agencies to manage crime-related information and other policing functions.]

Again the 43-force approach appears ill suited here, the fact is that each force can essentially choose to what extent and with whom they share data and IT systems, a decision often based on local friendships, politics or costs rather than overall effectiveness to combat crime.

One senior non policing official noted that one police force they were sharing with didn’t accept PDFs. Other issues included, the double or triple inputting of information highlighted by CID officers from a range of forces, which is obviously a huge waste of resources.

Furthermore, Hall (2021) provides an incredibly detailed assessment of Police IT capabilities in *Policing Insight* and further outlines the problems of the 43-force approach when considered from a data harmonisation standpoint and argues that ‘true harmonisation’ would also have its pitfalls.

“Every force has its own processes, procedures, databases etc. This autonomy is a part of their strength, so true standardisation and harmonisation across all forces is not the correct goal. “Interoperability via APIs [a way for 2 systems to talk to each other] and data standards is the more appropriate and realistic goal and is something policing is already working towards.

“This regional structure of UK policing isn’t changing, so its IT solutions have to work with this, not against it. We cannot have another national IT implementation failure which doesn’t work for anyone. It is better to work with what is already here.

“While some issues remain with accessing the back-end systems of certain police systems and incumbent suppliers sometimes being unwilling to share interface information, the opportunity for fast-paced innovation is certainly here in a way it wasn’t 15 years ago. Nowadays software can be written once and deployed with relative ease to most smartphones, tablets and laptops whereas 15 years ago ‘walled gardens’ between BlackBerry, Windows, and Nokia where a huge risk.

The law enforcement and policing nexus

One senior member of the UK Intellectual Property Office identified a series of challenges that the IPO, as non-police organisation faces in relating to sharing data on organised crime.

“After the creation of PND it ended up that serious and organised crime was defined by police as they saw it, without input from other agencies who deal with Serious Organised Crime (SOC) such as Customs, Trading Standards or the IPO. We haven’t got access to PND and that’s a big barrier for us. We rely on other partners to update the information for us.

“We can’t see the MoRiLE [Management of Risk in Law Enforcement] assessments across the UK regarding IP crime, unless we specifically request. But then if we don’t know it’s there how do we know to request it?

“We operate under a gateway [to share information] within the Enterprise Act. But the interpretation of those gateways is different. Customs interpret the same gateway completely differently to the way Trading Standards would interpret it. The police don’t go anywhere near the Enterprise Act for disseminations.

“It goes round and round and round. Whoever happens to be sitting in that chair at the time, their interpretation of that gateway, the interpretation of the quality of their data. That’s inevitable because we’ve never put intelligence sharing into a statutory format.

Case study 1: East Midlands

We did some work back in 2005 when we very first set up the Regional Intelligence Unit as a pilot in the East Midlands, because it was the first one of its kind in the country funded by the government.

We did some work with a company called Infoglide in America and they basically shipped over from Seattle some of their programmers, and we exported three datasets from three forces in the East Midlands, so we exported crime data, custody data, and then command and control data. So those three datasets were exported from each of the forces, and we put them into a standalone server, and Infoglide were then tasked to bring their scripters over and they wrote a script to interrogate the system.

Basically, the idea was to try and make it automated. You could use the nine databases as an interrogation tool if you wanted to, so you could dip into it and go, “I want to look for a red BMW in the ’88 year,” you will find all the red BMWs, but what we wanted to try and do is make it intuitive that it would identify patterns, trends, and connections in a live scenario. The reason that that company were asked to come, is because they had done the same in 2005 for the whole of the US. So, for their new Border Control Act in 2001 after the Twin Towers. So, they basically pooled 140 datasets, nationally significant datasets, and they were interrogating that, and also identifying patterns and trends for border control and homeland security. Ultimately, we were stopped from taking that further forward because of the transformation from what was INI into PND.

When you look at datasets and data sharing, it’s not about sharing all your data with everybody, is it? It’s about sharing your data in a common place where the right people at the right time with the right reason can access, either as an interrogation tool, or automated programming can find trends, and connections that would help in identifying or detecting crime.

If you had said to me, “Has Wales ROCU got automatic access into everything that the Eastern region does?” No, they haven’t. Is there currently an IT connection that enables that? No, there isn’t

Case study 2: Sharing information between UK forces

One Inspector at a large UK force spoke about the challenges of sharing information between force. We will get a bit of information. We will grade it 1 to 5, so A, B, C, D, E, 1, 2, 3, 4, 5, and then what we can do with it, that’s a national process. We will store that, on our force, in our form, in our way. What we can’t do is transfer that, electronically, into another force, if that makes sense.

So, say we get a bit of intelligence that ‘person a’ hoards child porn, or something like that. What you’d like to, I think, do is, take that report and give it to other forces so it loads straight into their system, and then they’ve got it.

No. What would happen is, we would have to take it out, and basically, put it into like an email, or a PDF, or something like that, send it to them as a PDF. They would have to then manually input the exact same information onto their form to upload it into their system. It’s just the fact that every force uses something different. Everyone does it in slightly different ways.

Say I had a proforma Word document, it won’t be the same as the other forces. So, someone will physically have to take the data from one and put it into the data on the other one, even though it says the exact same thing.

So, there is some slight barrier to that purely around resourcing. That’s two people; someone having to extract the data and put it onto a form. Someone in the next force will have to read the data and put it onto a form. So, you can see that builds in time delays and all the rest of it. So, there’s one blocker, if you like, around transferring information from force A to force B.

I don’t think it was ever that we didn’t want to share information. I, generally, think it was that we weren’t quite sure of the best way of doing it. PNC is a national database. NABIS is a national database. Intelligence isn’t. Of course, it’s accessing what’s on other people’s databases.

I get it all the time. A car comes into my force with a marker for firearms, say from the Met.

So, the Met will put on a marker, ‘This car is involved in crime.’ I don’t know what intelligence the Met holds on that car, because I’ll put it on my system, and it’ll probably come up with very little, because unless been linked with a crime in our force, I may know very little about it. I might go, ‘As far as I’m aware, there’s nothing on this car.’ What I have to do is, basically, I phone the Met and say, ‘Look, you’ve stuck this marker on. What do I need to know about it?’

Then you have sharing information with emergency services. That’s a massive problem Because we have it all the time the ambulance service will go to a job and they’ll go, ‘It says, on our system, that person X there is dangerous.” We’re like, ‘Really? Where has that come from?’.

Case study 3: Operation Venetic

One former inspector at a large urban force, notes some of the antiquated ways methods that were still being used to sort data and how that reflects on policing’s overall capacity to deal with this issue effectively

*When we first had the Venetic data, the plan was I s*** you not to print it all off lock people in a room together and get them to highlight the conversations. I was like Are you kidding me? We are in 2020, and you are suggesting that we print this off, print it off so we have copies of this, and we highlight it with highlighter pens., honestly.”*

I was like, “Well, one of the techies they can build that within a key word search platform for you within probably a week.” They were like, “What?” Sure enough, within a week we had converted it into something that could ingest it and search. You are talking thousands and thousands and thousands of sheets of paper which that you’ve got to then keep secure. I was just gobsmacked.

One officer with current national organised crime policing experience echoes these experiences. "When Venetic came along, we were putting memory sticks in cars and motorbikes and driving up the M1 to share data because we couldn't move secret data across the policing network.

The new Venetic that's come out, the data server, again we weren't even at the table. We weren't even invited. The Dutch have again acted by proxy as our representative. The Dutch are taking all the material and then the Dutch are managing it with us. We have a really good relationship with the Dutch.

Given that, when compared globally the UK is in the top bracket of technologically and economically developed countries and is plagued with issues like this, what hope to do those member states with less infrastructure and less funding have?

Law enforcement capabilities in developing countries

In the previous section, we have looked at how the developed countries, with all their resources, handle the challenges of 21st century digital policing. Now we come to the countries with much bigger organised crime problems and much less capacity to tackle them.

One former detective specialising in organised crime who now operates in the private sector at a global level, argues that commonly held tropes around the financial disparities between the two groups of countries is not the only factor.

*"*The mentality needs to be that the understanding, it needs to be understanding at geopolitical level. Not all cultures, and most countries do not operate in the same way. Either, culturally, jurisdictionally methodologically, in terms of topologies, in terms of knowledge sets, the budgets that they have, the way that they operate, the individuals that the police forces are drawn from.

"So, police are not police are not police. Some that I have met don't even have shoes. They might not have a radio; they might not have phones. I once spoke to an individual who was the commissioner of an agency within Myanmar.

"They were getting paid as the Commissioner, the highest person within that organisation, 400 US dollars a month. So that gives you an idea of why organised crime works. It works because police in one country is not the same as police in another country. Standards vary hugely across the world.

"I've been in countries where the officers have had no shoes, they've had no cell phone, they've had no transportation. What type of either response mechanism or detection mechanism is that police force likely to have? Zero. It also leads to corruption. It leads to bribery.

Case Study 4: Balkans

One former UNODC Head of Station in the Balkans identifies both financial and governance challenges in his former region. "The borders (in Balkans) are incredibly corrupt, incredibly corrupt. And obviously, with that level of corruption comes a level of unprofessionalism. Part of the issue is that they don't get paid. The money you earn as a law enforcement, or even a public official, even a prosecutor or a judge, it's just not enough to really- it doesn't keep the talent.

The other issue is bureaucracy, a senior- let's call them a senior investigation officer, an SIO, as UK policing would know it, does not have the authority to share anything with anybody. There's no devolution of authority. There's no devolved authority.

For example, to if, as UNODC, I send a letter inviting, I don't know, let's pick Serbia, to select five officers to attend a training in Turkey. That will require 12 signatures, and the last signature will be the interior minister. Just to allow five officers- not of any grade, this could just be five standard border police officers. So, low-ranked, but capacity-building training, 12 signatures. So, there's no, for example, inspector grade, which would be considered somebody with authority in UK policing. It can't be signed and say, "Yes, you guys can go. My two from my team are authorised to go."

There is not even a chief inspector or superintendent level person who has authority. They're just one, two, three of the twelve signatures required. So, you can imagine, I mean, it's a great example because when it comes to the question of intelligence sharing, you can already see the challenges

He also talks about the power organised crime wields in these areas and the challenges that brings when tackling them.

"They are integrated into society in a much deeper way than most Western Democracies- with the exception of Italy. A few years ago, the Prime Minister of Serbia was a guy called Đinđić. He was seen as a reformist, seen as somebody who was seriously going to tackle crime and corruption, and he didn't last very long. He was assassinated pretty damn quickly in his tenure, by organised crime.

"So, there's a real risk for those that really want to talk about it, and to really tackle the problems. You've got to be brave; you've got to be protected. And be realistic about your life expectancy."

Europol and Interpol

Europol and Interpol are both international organisations that help law enforcement agencies in different countries work together to fight crime. However, they have distinct focuses and geographical scopes.

Europol concentrates on the European Union and its member states. It supports these countries in tackling serious international crime and terrorism by facilitating the exchange of information and intelligence between national law enforcement agencies. Europol also provides operational support to investigations and joint operations, making cross-border investigations more efficient.

Interpol, on the other hand, is a global organisation with 195 member countries. It enables police forces across the world to collaborate in combating international crime. Interpol provides a platform for the exchange of information and best practices, and it issues notices and alerts to help locate and apprehend fugitives.

Although internationally, the Europol Information System (2022) and Interpol's nineteen different databases (2022) both hold significant tranches of information and facilitate data sharing and analysis on a huge scale, there has been very little systematic research designed to capture capabilities that can be provided by harmonising data between these resources.

As one US Interpol Operations Director suggested "one risk is if you are focussing on how things are done now and what is possible, we may not even know what is possible; so, part of this is dreaming outside the box; in a perfect world what could this system do?"

However, Brexit has impacted the benefits of international data harmonisation – One interviewee with international experience described it as a 'deep negative impact.' Another practitioner suggests that the UK was one of the biggest net contributors of information to Schengen Information System (SIS II), the Europol system and the UK was very active exchanging information across Europe and all the information that they supplied initially became practically and legally unavailable to Europol and vice-versa.

The US respondent is relevant for two reasons. In the first place the practitioner is looking realistically to the medium term to assess what is possible once the manual processes of the organisation are re-engineered with the supply of future benefits of new processes. In the second place, there is an element of separateness in that the US sponsor is outside the European union 'looking-in', in the same way as UK, post-Brexit falls outside the European union.

Operational Risks

Europol respondents suggest that US information is also shared between members across the Europol platform, One Europol official notes “the biggest liaison office we have is the US liaison office”. The key risk is how UK potentially aligns with the strategic vision of Europol and Interpol and how UK can have its voice in a fluid situation when sitting outside Europol’s and Interpol’s clear missions.

The possibility of deploying progressive data-centric strategies across borders after Brexit introduces a new layer of tensions for key UK personnel attempting to harmonise with European colleagues across borders and share intelligence across specialist databases. The risk is that UK cannot contribute directly to progressive thinking in this area and in a sense, UK becomes its own silo. This point is repeated by practitioners in that it makes data harmonisation in itself more difficult as it is already a ‘complex ask’ requiring the consolidation of multiple and complex technical resources but also combining human factors across diverse political, legal and jurisdictional spectra.

Harmonisation of Case Management Systems at Interpol Washington U.S. National Central Bureau

The key harmonisation benefit concerned the case management system with the harmonisation of automated manual tasks especially across time-consuming manual indexing activities. Here there are human computer interaction benefits that can be accrued to the international Interpol system. Such rationalisation can be improved with enhanced logging-in procedures. The harmonisation of Department of Justice must have various legal protocols when other systems that are plugged in such as FBI.

Harmonisation can sort out tensions in systems such as de-confliction issues making data acquisition and ownership more explicit and more transparent. Transformation might be obtained through business process optimisation - a capability that requires new human skills’ sets and to be identified early in the design and configuration of the solution. ‘The policy needs to drive the tech and not the other way around.’

As one interviewee put it: “Essentially, the value of international data harmonisation is the accumulation of large datasets beyond what would normally be held within one organisation or entity containing many different aspects of information within the data set”.

Joint Investigation Teams (JIT’s): Data harmonisation on a project-by-project basis?

Joint Investigation Teams (JITs) are deployed on a pan- European basis and facilitated by Europol (Eurojust 2020) These projects enable two or more countries to pool resources, and coordinate, cooperate and develop expertise during an inquiry that affects both/all countries.

There are examples of significant wins against organised crime based on the JIT approach. Of note is Europol-supported joint investigation team, (Europarl 2021)- code named Emma 95 in France- that infiltrated and then ultimately closed the *EncroChat* encrypted phone system after the gathering in real time of millions of messages between suspects. Information was also shared with law enforcement in several countries that were not participating in the JIT, including the UK, Sweden and Norway.

Subsequently, the National Crime Agency (NCA 2020) responded to the 10,000 users in the UK (2020) with Operation Venetic. UK police arrested 746 individuals, including major crime bosses, intercepted two tonnes of drugs (with a street value at the time in excess of £100 million), seized £54 million in cash, as well as weapons. The NCA said that 2,631 people had been arrested in the UK as part of Operation Venetic; 1,384 had been charged, 260 convicted and over five and a half tons of class A drugs, 165 weapons and £75m in criminal cash was seized.

Similarly, Operation Eureka involved a JIT that led to arrests of 108 people suspected of being involved with 'Ndrangheta in Italy (Henley 2023) with more than 30 arrests in Germany after four years of investigations.

As a final example, in 2015 (Europol 2015) a major cybercrime ring using malware to attack online banking systems was dismantled by a JIT and was described by then Europol Head Rob Wainwright ‘one of the most significant operations coordinated by the agency in recent years by Europol. The JIT consisting of investigators and judicial authorities from six different European countries, targeted high-level cybercriminals and their accomplices who are suspected of developing, exploiting, and distributing Zeus and SpyEye malware.

The damage produced by the group is estimated to be at least EUR 2 million. One Interviewee, a member of Eurojust, noted “This case demonstrates that it is only possible to combat cybercrime in a successful and sustainable way if all actors-that means investigative judges and judicial authorities- coordinate and cooperate across the borders.’’

JITs: The way forward for cybercrime investigations?

JITs are a way for law enforcement and prosecution officers from different jurisdictions to communicate over a specific case for specified period. In terms of speed, they are much more efficient than the system of International Letters of Request they replaced;

however, they are not a ‘Skeleton key to access information’ and there are still challenges around their implication.

Hunton (2010:85) A specialist in computer forensics introduces the key risk of failing to harmonise when he argues that a ‘Distinct lack of any single definitive cybercrime investigation model’ both for the UK and Europe is hindering police investigation into the topic and, because of the way cybercrime spans borders, that any model must be flexible enough to allow straight forward multi-jurisdictional investigations.

On a European level, each Member State has its own laws governing collection and retention of evidence- which means evidence gathered in one country may not be valid in another. Given how easily cybercrime transcends borders law enforcement’s inability to do the same is a disadvantage. This in effect requires international cooperation and harmonisation of procedures and guidelines to combat and prosecute cybercrime as well as undertaking technical harmonisation.

One of the challenges around any DH approach is one of legal and jurisdictional knowledge. Essentially, officers have knowledge of their own jurisdiction but not of others and until that changes Cybercriminals’ ability to transcend borders almost instantly, while law enforcement are both mired in process and still attempting to obtain the requisite skills, will mean the criminals will maintain a constant advantage.

The ‘ideal scenario’ is that UK develops a specific matrix force harmonised with European partners on a case-by-case basis with specific investigatory targets. One party suggested that there is a place for another trust-oriented international crime bureau- that would sit as a separate entity and be defined specifically by its neutrality so that it works outside current political systems. It is ‘as independent as possible’.

Case Study 5: Cloud storage and legality

You can’t talk about Data Harmonisation without considering the challenges around storage and access of data, for a true harmonisation approach you either need all of the data you want to analyse to be in one big pot (the cloud) or you need permission to run a pipeline into each database that can search for the information you want (an API).

Corporations such as Amazon and Microsoft have been leaders in the cloud world since its inception and UK policing currently has vast chunks of data stored through agreements with Microsoft and Amazon for the use of seemingly basic services such as Teams, the problem is that the companies are American and therefore the data may be stored on American soil, which is problematic from a legal point of view.

One interviewee with a specific data protection background in the UK, spoke about the challenges around dealing with big corporations from a public sector perspective.

“The first thing that struck me was that Microsoft won’t issue a specific contract. I find it a very bizarre situation. Anything else that you procure, you issue the contract. When you’re buying services, you issue the contract. With the Hyper-Cloud, hyperscale cloud providers, they’re issuing their standard terms and conditions to you. Your standard terms and conditions are the same for everybody.

“That’s a problem when it comes to Part 3 of the Data Protection Act because there are a number of sections in Part 3 of the Data Protection Act, that require there to be things in the contract. Obviously, they’re not there in the standard contractual terms of Microsoft.

“It makes a couple of statements that raised red flags for me, like, ‘it’s not suitable for high-risk processing’. And it says, ‘You will indemnify us if you process high-risk processing’ Well, we’re about to put all our pending cases onto it. We asked Microsoft Can you confirm that Azure is compliant with Part 3?” And the response was, “We’ll need to take legal advice, and this will take some time.” That does not fill me with confidence.

“So, everyone thinks it’s okay to put all this data in the cloud and have Microsoft move it about because it’s encrypted. But most of the solutions that we’ve looked at, that people are using, involve Microsoft caching the key. Microsoft will have your key. So, if they should get a request from the American government, there will be points of time during their process on that data, they will have the key to unlock that data.

“Now, we know Microsoft push back against requests from the American government. We know Axon would push back but at the end of the day, they can be compelled to release that data to the American authorities. So, we’re saying to ourselves, “Right. If there was another Lockerbie…”

“We had some moments with the Americans at Lockerbie, because the victims were largely, their citizens on that plane. US authorities would probably have liked information a lot earlier than we were prepared to provide it.

“If that happened again, would they just go, “Right.” So, would it all be in this database? “We’ll just go and compel Microsoft to give us this, from Azure.” So, while that risk is probably really low, the impact, should that happen once for a major investigation, is massive.

“Microsoft’s quite vague about its data processors. It can add new data processors at any time it likes, and it will tell you and your only remedy if you don’t like the data processor is to end your contract. That’s not really a remedy. If they come and tell me, “Oh this processor from Brazil’s going to come in.” And we’re, “That’s not suitable for us.” Our remedy is to end the contract.

“That’s not going to work for us, given that our desktops and everything are… They’ve, kind of, got us over a barrel because we’ve purchased. We’ve spent the money.

“There’s maybe, one provider in the UK, cloud provider that meets all the sovereign data requirements. But I don’t believe, certainly not at this point in time, they’ve got the capacity to take all the processing that’s currently being done, that Microsoft are handling for the police.

“I think forces in England and Wales appear to me, to have looked at products and said, “Oh, they’re on G-Cloud [UK Government purchasing hub]. We can use them. Just because they’re on G-Cloud doesn’t mean they’re suitable for law enforcement processing.

“Part of the problem is the US legislation The CLOUD Act in the US. It allows the American government to require Microsoft to provide the data to them, wherever that data is. If it’s in a data centre in the UK, the American government can require Microsoft to provide it to them.

“The CLOUD Act came about when Microsoft refused to give the American government data that was in a data centre in Ireland. So, what did the American government do? Brought in legislation.

“Do I think it’s fixable? Yes. Fairly easily, if we can get Microsoft to the table and have them accept that there are a group of customers that spend quite a lot of money with them. Axon want to fix this. Axon [provide a lot of body worn video services to UK forces] have told us they’re Microsoft’s biggest customer in the UK. They get the issue. They’re keen to resolve it.

“So, they’re happy to lobby with us, to Microsoft, to say, “Look. You’re making a lot of money from the police forces in the UK. So, we feel that you do need to change your standard contractual terms for this data. You will have to give us guarantees, written guarantees that that data won’t go outside the UK but won’t be accessed from outside the UK.

Another interviewee, who has been heavily involved in the design and implementation of policing databases over the last two decades, is unequivocal when discussing the legality of UK policing’s move to the cloud.

“The police are operating under Data Protection Act Part 3 and the two bits of legislation (Data Protection Act or GDPR) don’t match up against one another. They don’t mesh, rather. That’s the fundamental background problem. Now, when the UK left Europe, from 1st January 2020, from that point forward, it was very hard… Not impossible but really tremendously hard for that data ever to leave the UK, for either processing purposes or to be shared with another agency.

“Under post-Brexit rules, sending data to Jersey, Guernsey and Isle of Man is an international transfer and therefore, really, really hard to do. Yet, they’ve got day-to-day access to PND and PNC. So, every time they access that, that’s actually an international transfer and has to be managed a particular way and it’s not being managed that way. So, that’s another area of problem.

“The legislation exists to protect data subject’s rights. If the technology that you are using requires you to change the law, you’ve picked the wrong technology.

Conclusion and Recommendations

This paper has consistently highlighted the difficulties in countering organised crime. These challenges arise from the diverse standards, priorities, and resources among EU Member States, coupled with the varied nature of criminal activity and organised crime structures.

Harmonising data can significantly improve the fight against organised crime. Firstly, it leads to more effective international investigations by allowing efficient cross-border data sharing. This allows skilled police officers working in joint investigative teams to access and analyse information quickly, using a common terminology. Secondly, creating specialised systems that allow access to existing databases across different countries provides a more comprehensive view of criminal activity. This increased access to information can be vital in identifying and disrupting organised crime groups.

Data Harmonisation offers significant benefits in the fight against organised crime. It provides advanced analytical capacity, allowing investigators to 'join the dots' and gain enhanced insights. By providing access to a richer and more complete dataset, including historical context, it gives investigators an operational advantage and improves team situational awareness during operations.

Currently, investigators often rely on keyword searches in police databases, requiring them to guess every possible synonym for a topic. This makes it difficult to collate and cross-reference information from different international sources. A standardised lexicon would solve this problem and enable the development of effective text-mining software.

Artificial Intelligence offers a broader approach, capturing diverse data not limited to crime systems. By pulling in information from non-specialist sources, it builds a richer picture of the criminal context. This convergence of technology creates new demands for law enforcement, allowing for a more integrated view of information and increased efficiency. However, it also presents a risk: if UK law enforcement remains outside these processes for managing large-scale IT systems in the areas of freedom, security, and justice, it will become less effective in combating organised crime and will be sidelined as a key contributor and receiver of information.

There are multiple barriers to a 'one database fits all' approach to intelligence sharing. Firstly, even in developed nations like the UK, sharing data effectively within and between forces, let alone internationally, is a huge challenge. While systems like the organised crime group mapping system exist, they operate on a very basic level. Devising a solution that surpasses the current capabilities of agencies like Europol or Interpol is a significant undertaking.

Secondly, many countries lack the policing capabilities of developed nations. For example, a cybercrime unit in an African country may lack basic resources like computers, making data harmonisation a low priority. Similarly, nations that are still developing economically and act as strongholds for organised crime, such as Macedonia, lack the necessary national intelligence infrastructure to participate in data harmonisation efforts. While the UK also lacks a single national intelligence system, its capacity to share and analyse data far exceeds that of less developed countries.

One interviewee involved in law enforcement in the UK notes “the theory of Interpol is that there is a free exchange of intelligence through national central bureaus, but you know, people are very guarded what they send. It’s ended up becoming a message passing system. That’s not an intelligence system.”

Another senior police officer with current organised crime operational experience, argues that the ultimate solution would be if everyone would be on the same system.

“That would be a massive win. But we are not. We are on, we are not on 43 different versions, but we are on probably 8 or 9 different versions. If we look at Niche, most forces tend to be using Niche Record Management System. They are all on different variants as well, so a lot of them don’t talk to each other.

“If I could design a new system, I would look at the Scottish model [eight regional forces merged into 1 force in 2013], but then look to get everyone on the same IT.”

“the next link twist to that, is that most of the risks that we have around live investigations, they involve a lot of foreign national offenders. Since we’ve lost access to Schengen post-Brexit our only opportunity to get access and for searching on European datasets is via PND.

“If it’s not on PND we are not going to pick up any markers, any intelligence around firearms, or significant risk. At the moment the only material we have brokered by Interpol. We fire our PND into Europol. Europol then run it through an agreement with Interpol, because we are persona non grata to a certain extent in Europol now.”

Recommendations for Effective Data Harmonisation

1. Transform Organised Crime Group (OCG) Mapping into a National Intelligence Hub:
   - Significantly expand the scope and functionality of OCG Mapping to create a single, comprehensive source of OCG intelligence for all UK law enforcement agencies. This will improve collaboration and intelligence sharing, enabling a more coordinated and effective response to organised crime.
2. Establish a Unified National Body to Combat Organised Crime:
   - Consolidate organised crime responsibilities currently divided between the National Crime Agency and Regional Organised Crime Units into a single, powerful national body. This would streamline operations, eliminate jurisdictional barriers, and foster a cohesive approach to tackling organised crime across the country.
3. Resolve Legal Barriers to Cloud Adoption:
   - Conduct a comprehensive review of legal and regulatory issues surrounding cloud computing within UK policing. Address these challenges to pave the way for secure and efficient data storage and access, enabling effective data harmonisation across different platforms and systems.
4. Develop a Specialist Cadre of Data-Savvy Investigators:
   - Implement a new training and recruitment programme to create a dedicated cadre of officers skilled in navigating multiple systems and digital media investigations. These specialists will be equipped to leverage sophisticated analytical tools and maximise the potential of data harmonisation for complex investigations.
5. Foster Trust and Collaboration through Formal Agreements:
   - Establish a formal agreement between stakeholders and agencies to address the existing trust deficit. This agreement should clearly define roles, responsibilities, data access protocols, and information sharing frameworks, ensuring transparency and accountability within the data harmonisation process.
6. Standardise Terminology for International Compatibility:
   - Develop a standardised glossary of common terminology for data entry into police databases. This glossary should be adopted nationally and aligned with international standards to facilitate seamless information exchange and collaboration with international law enforcement agencies.

Please contact Dr Chris Allen on Chris@criminis.co.uk for further discussion

References

Allen C (2021) Solving organised crime: What is the way forward for international co-operation? https://policinginsight.com/features/analysis/solving-organised-crime-what-is-the-way-forward-for-international-co-operation/

Allen C (2023*) Investigating organised crime - perspectives from within the police: A case study on business techniques and how can they be applied to analysing OCGs in a police setting*. Liverpool John Moores University

CEPOL (2022) Available at https://conference-digital.cepol.europa.eu/cepol-research-science-conference-2021-mru-vilnius/schedule/

CoPaCC (2019) Forces in Focus: Comparing User Experiences. An in-depth comparison of the 10 forces providing the largest survey response in 2018. Available at https://policinginsight.com/wp-content/uploads/2019/12/CoPaCC-Police-ICT-Forces-in-Focus.pdf

Eurojust (2020) *Third JIT Evaluation Report* Available from: Third JIT Evaluation Report | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu)

European Parliament (2021) Parliamentary question - E-003454/2021. Available from https://www.europarl.europa.eu/doceo/document/E-9-2021-003454_EN.html

Europol (2015) *Major Cybercrime ring dismantled by Joint Investigation Team*. Available from https://www.europol.europa.eu/media-press/newsroom/news/major-cybercrime-ring-dismantled-joint-investigation-team

Europol (2017) *Serious Organised Crime Threat Assessment*(SOCTA)) definition of OCG NP [Online] available from https://www.europol.europa.eu/socta/2017/key-judgments.html

Europol (2020) *Europol's Amended Regulation Enters into Force*[online] available at https://www.europol.europa.eu/media-press/newsroom/news/europols-amended-regulation-enters-force

Europol (2022) *The Europol Information System*. Available at https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system

Europol (2023) *Processing of Personal Data*. available at Processing of personal data | Europol (europa.eu)Europol (2023) *Rules of Processing Data* 2020 [online] available at https://www.europol.europa.eu/processing-of-personal-data

Europol (2023) Secure Information Exchange Network Application [online] Available at https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena

Hall S (2021) Policing Insight. Available at: Fifteen years and counting: Revisiting the predictions for police IT from 2006 - Policing Insight

Henley J (2023) Guardian Newspaper *Police detain 130 in raids across Europe targeting 'Ndrangheta mafia. Available from* Police detain 130 in raids across Europe targeting 'Ndrangheta mafia | Mafia | The Guardian

His Majesties Inspectorate of Constabulary and Fire and Rescue Services (2021) *Regional Organised Crime Units: An inspection of the effectiveness of the Regional Organised Crime Units.* Available at Regional Organised Crime Units: An inspection of the effectiveness of the Regional Organised Crime Units - HMICFRS (justiceinspectorates.gov.uk)

His Majesty's Inspectorate of Constabulary Fire and Rescue Service (2020). *An inspection of the National Crime Agency's criminal intelligence function*. Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/publications/an-inspection-of-the-national-crime-agencys-criminal-intelligence-function/2020

Home Office (2018) Serious and Organised Crime Strategy

Home Office (2022) *UK US data access agreement factsheet*

https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet

Hunton, P. (2010). Cyber Crime and Security: A New Model of Law Enforcement Investigation. Policing: A Journal of Policy and Practice, Volume 4(4), pp.385–395.

Interpol (2017) summary of organised and emerging crime strategy. Lyon

Interpol (2019) *Organised Crime [Online] available from* https://www.interpol.int/Crime-areas/Organized-crime/Organized-crime

Interpol (2019)https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-reviews-its-rules-for-the-international-exchange-of-criminal-data

Interpol (2023) *Interpol databases [Online] available from* https://www.interpol.int/en/Who-we-are/Our-history/Key-dates

Interpol (2023) *Interpol reviews its rules for the international exchange of data [Online] available from* INTERPOL reviews its rules for the international exchange of criminal data

Interpol (2023) *Project IDEA [Online] available from* Project IDEA (interpol.int)

Interpol (2023) *Project Insight [Online] available from* Insight (interpol.int)

Kennedy R (2020) Euronews. *EU authorities penetrate phone network in huge, organised crime sting*. Available from: EncroChat: European authorities compromise phone network to arrest 'untouchable' criminals in sting | Euronews

National Crime Agency (2019) National Strategic Threat assessment. London

National Crime Agency (2020) *NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation*. Available from: NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation - National Crime Agency

Occhipinti John D (2015) Still Moving Toward a European FBI? Re-Examining the Politics of EU Police Cooperation, Intelligence and National Security, 30:2-3, 234-258,

Royal United Services Institute, Babuta A (2017) Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities, London

Royal United Services Institute, Babuta A (2018) Whitehall report 3-18 Machine Learning algorithms and police decision making legal ethical and regulatory challenges, London

The Police Foundation (2017) The impact of organised crime in local communities

UN office on Drugs and Crime (2010) The Globalization of Crime: A Transnational Organized Crime Threat Assessment [online] available from < https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf> [20/12/2016]

University of Michigan (2022) Available at https://www.icpsr.umich.edu/web/pages/DSDR/harmonization.html#:~:text=Data%20harmonization%20refers%20to%20all,of%20data%20from%20different%20studies.

Wainwright T (2016) *Narconomics: How to run a drug cartel*. London: Ebury press

Wright R (2018) National Crime Agency Deputy National OGM Manager- PowerPoint on organised crime group mapping processes sent to author May 2018.

Wright R (2020) The Financial Times. *Hundreds arrested across Europe as French police crack encrypted network". Available from* Hundreds arrested across Europe as French police crack encrypted network | Financial Times (ft.com)

Ye J (2021) *the Slippery slope of Big data in policing. Harvard International Review.* Available at: https://hir.harvard.edu/big-data-in-policing/

Project Morpheus:
Examining the potential to utilise data harmonisation to enhance international organised crime policing capabilities

An Oxon Advisory ‘Emerging Technologies and Strategies for Public Safety’ Series Report

www.oxonadvisory.com