Policing: an International J

# Does Information Communication Technology facilitate or solve crime? Exploring the experience of law enforcement practitioners in three countries



| | |
|---|---|
| Journal: | *Policing: An International Journal* |
| Manuscript ID | PIJPSM-07-2024-0103.R3 |
| Manuscript Type: | Research Paper |
| Keywords: | information communication technology (ICT), Information sharing, intelligence, Law Enforcement, serious organised crime (SOC), multi-agency |
| | |

# Does Information Communication Technology facilitate or solve crime? Exploring the experience of law enforcement practitioners in three countries.


## ABSTRACT

**Purpose**: The frequency, harm and reach of transnational serious organised crime (SOC) is increasing. This study examines how Information Communication Technology (ICT) has facilitated this type of crime and has been used by law enforcement agencies to tackle it.

**Design/methodology/approach**: 62 law enforcement practitioners, from the UK, Australia and New Zealand, who had experience of tackling SOC through intelligence-led approaches were interviewed. Following thematic analysis of the semi-structured interviews four themes were highlighted.

**Findings**: The study found a high degree of practitioner consensus across the UK, Australia and New Zealand on four points. First, SOC had become more transnational, significantly increasing in frequency and diversity. Second, this trajectory had been facilitated using ICT. Third, law enforcement practitioners were using ICT to improve the detection and disruption of SOC offenders. Finally, the potential of ICT was not being maximised by law enforcement as practice continued to rely heavily on manual processes and human relationships. The reasons behind this trend were explored.

**Originality:** It is the first to show law enforcement agencies across three countries share similar organisational and individual behaviour concerning information management practice when engaged on intelligence-led approaches. It suggests new ways to enhance effectiveness and efficiency of approach.

## INTRODUCTION

Information Communication Technology (ICT) can be understood as technology that "helps to produce, store, transmit, communicate and/or disseminate information in all forms, including voice, text, data, graphics and video" (Nuth, 2008, p.439). ICT has always been associated with crime in both positive and negative ways. For offenders, ICT has acted as a general crime facilitator (i.e. enabling individuals to forge new identities), generated new offences (i.e. computer misuse, cyber-stalking), and allowed old crimes to be committed in new ways (i.e. deception, counterfeiting). For law enforcement agencies, ICT has been at the forefront of intelligence-led approaches. Approximately 6% of the population are thought to commit 60% of all crime (Ratcliffe, 2016), whilst 3-6% of hot spots (individual addresses and street segments) suffer 50% of crime (Sherman, 1995; Weisburd, 2015). Targeting the most criminogenic people and places, through an intelligence-led approach, is the most cost-effective way of reducing crime. Generating the information to facilitate their identification and behaviour is critical. The purpose of this study is to explore whether law enforcement practitioners are maximising the potential of ICT to tackle serious organised crime (SOC).

### Literature Review

As Routine Activity Theory argues, crime can emerge as the intentional consequence of unintended opportunity and technological advances play a significant part in this (Farrell and Tilley, 2017). Such innovation regularly outpaces the speed in which governments can legislate. Physical travel is now faster and more economical, allowing more opportunities to offend (Europol, 2017; Lück *et al.*, 2006). In the UK, foreign nationals comprise between 11-20% of those arrested or imprisoned (Beckford, 2018). Similarly, the exponential use of the internet increasingly intersects with the physical world (Schwab, 2015), with approximately 63% of the world population online (Bartley, 2023). This allows offenders greater access to vulnerable victims and the ability to commit crime from remote locations using deception and disguise. As a result, online crime has risen dramatically and SOC has become increasingly recognised as transnational (Australian Criminal Intelligence Commission [ACIC], 2017; Barker, 2019). Articles across the UK, the European Union, Australasia, North America, and South America have commented upon the growth of SOC, both in the number of offenders and the level of harm (ACIC, 2017, 2021; Europol, 2017, 2021; Global Initiative Against Transnational Organized Crime, 2023; Haenlein and Lord Evans, 2023). The cost to society has also increased significantly; indeed, a single computer worm in 2004 was estimated to cost international business US $38b (Gerencer, 2020). To respond, nations have invested more effort and resources into tackling the problem.

SOC offenders are well placed to innovate as they lack the constraint that can stifle law enforcement agencies. Carrying only individual responsibility and accountability, they are unhindered by legislation or a moral code. Generally, SOC offenders are entrepreneurial and favour social networks, rather than hierarchies (Gottschalk, 2009). This allows offenders to remain flexible and follow opportunities, joining with others or working alone. They are

unrestricted by physical or virtual boundaries and able to acquire any tool or technology that facilitates their aim. In this way, ICT has assisted in providing SOC offenders with competitively priced encrypted video and speech communication (Napoleon *et al.*, 2021). This allows them to access criminal contacts and goods anonymously, using facilitators such as the dark web and cryptocurrency.

How then can law enforcement tackle the threat? A starting point is deterrence theory, which emerged with the writings of Beccaria in the 18th Century, before becoming mainstream in the 1960s and 1970s (Chiricos and Waldo, 1970; Gibbs, 1968). Its core principle is that offenders seek to maximise reward and reduce loss. Therefore, if the behaviour (i.e. crime) is believed to bring a likely sanction (formal or informal) then the behaviour is less likely to be conducted. This is especially true if the sanction is thought to be significant and delivered in a fast and reliable way. Developing this theme, Rational Choice Theory (Cornish and Clarke, 1986) argues that by increasing offender effort to commit the crime, or by increasing their risk of detection, offenders can be deterred. Technology has played a major role in this process, originating with fingerprinting which emerged in the late 19th Century (Broeders, 2007). Innovation has accelerated in the 21st Century. Developments such as Automatic Number Plate Recognition (ANPR) can connect a vehicle with various databases to establish ownership, location and travel patterns. This has assisted in the detection and reduction of crimes, including murder and armed robbery (Kirby and Turner, 2007). More recently, facial recognition is being developed to enhance the effectiveness of ubiquitous CCTV cameras.

Digitisation provides the opportunity to connect with a global network of law enforcement practitioners and extensive intelligence systems. It also provides the ability to track criminal behaviour through a myriad of electronic traces. This may include purchases (bank cards, loyalty cards, financial records), efforts to access or post information (utilising smart devices or social media) or travel (satellite navigation systems, ANPR or CCTV) (Ferguson, 2017, p.9). Indeed, the potential of accessing open-source information has been regularly illustrated in investigative journalism. In a high-profile case, Bellingcat (a collaboration of independent journalists) outperformed government resources by identifying the Russian nationals responsible for the Novichok poisoning of Sergei and Yulia Skripal (Bellingcat, 2018). The technology exists to search a myriad of databases simultaneously using open-source intelligence techniques.

The ability to manage bulk data is becoming increasingly important in a world where 90% of all data has been generated in the past two years (Bartley, 2023). These trends are expected to continue as more people conduct business online (ONS, 2021). Indeed, the ability to use data science and artificial intelligence (AI) is increasingly emphasised in the field of national security (Babuta *et al.*, 2020; Niels, 2023). Similarly, data analytics conducted at either individual, group or population level, in full or semi-automatic formats, can outperform

human analysts in both scale and speed. More recently, behavioural analytics, which incorporates data analytics with behavioural science, generates further insight by identifying links not immediately apparent to the human eye. At its most sophisticated level it could involve forecasting or predicting future behaviour by analysing patterns of past behaviour (Babuta *et al.*, 2020; Harris *et al.*, 2023). This latter benefit is supported by considerable research which shows that individual behaviour (including offenders), is often predictable (Brantingham and Brantingham, 1984; Canter and Gregory, 1994; Rossmo, 2000). In fact, behavioural predictability has been discovered in social interactions, shopping, mobility, and online behaviour (Song *et al.*, 2010; Zhang *et al.*, 2021). As such, the use of behavioural analytics can both save resources and produce investigative leads which otherwise may be missed.

The critical question arises as to whether law enforcement agencies can operationalise this technology to deliver its potential (Birkinshaw, 2014). Several factors are said to be responsible for intelligence failures, which are regularly reported (Taylor and Russel, 2012). First, it is suggested information sharing is prevented due to the prevalence of incompatible hardware and software systems within organisations. Further, it is cited that law enforcement practitioners are constrained by having to comply with legislation and protocols surrounding information sharing regulation (Bradford *et al.*, 2018; Tyler, 2006) and investigative standards (i.e. Police and Criminal Evidence Act). The third issue relates to human factors. Whilst law enforcement organisations are rigid and hierarchical, individual practitioners are allowed considerable discretion in the actions they take (Banton, 1964; Fielding, 2002). Commentators have highlighted the inherent challenges associated with organisational and individual cooperation when conducted across a fragmented landscape (Carter, 2015; Carter *et al.*, 2016). They point out that even within law enforcement organisations, there exists a diverse range of roles and priorities which can facilitate or hamper the management and sharing of information. Ratcliffe (2016) also emphasises the role of human relationships in all aspects of intelligence-led policing, including the importance leaders have in valuing intelligence.

More recently, Phythian *et al.* (2024) provided further detail in understanding how human factors affect information management. By surveying 73 UK practitioners they discovered four main approaches of sharing information, distinguished by the level of human or technological effort required. In the UK, the most advanced technological approach is the Police National Database (PND), which allows any search term to be scanned across 230+ separate police databases, allowing suitably authorised practitioners to obtain a more complete intelligence picture. However, the study found this type of system was used infrequently, with practitioners more likely to rely on trusted human relationships through the manual circulation and development of information. The study also found the sharing and analysis of data becomes more problematic the more distant it becomes conceptually (i.e. when being passed outside the law enforcement environment) or physically (i.e. across

international borders). Other studies have highlighted international challenges citing practical issues such as language, legal systems and hardware (Birdi *et al*., 2020). In these contexts, the data transfer is less likely to be automated, and go through physical clearing houses (i.e. Europol, Interpol) which increases bureaucracy, cost and time. Even if information sharing agreements are in place it relies on system owners deciding what information should be provided and for what purpose. This often means the criminal behaviour is already known, rather than the analysis proactively identifying patterns of criminality.

In summary, this literature review illustrated how transformative technological advances in ICT have been embraced by offenders engaged in organised crime. This has allowed them to obtain a competitive advantage, which has resulted in organised crime being described as more frequent, harmful and transnational in nature, often reported to be a government priority. Historically, commentators have been critical in the way law enforcement agencies have responded in terms of information management, citing that intelligence failure is inevitable (Wirtz, 2023). Existing literature has identified deficiencies caused by fragmented systems and human factors but the research often lacks detail. This has resulted in solutions often delivering more of the same (i.e. fusion centres), rather than transforming effectiveness and efficiency in a cost effective manner. This transnational research study seeks to examine this topic in more detail. It offers perspectives from practitioners based in three different countries, to ground current academic and theoretical understanding in empirical international practice. From a criminality perspective, it enhances existing understanding of the increasingly transnational and technology-facilitated nature of organised crime. From a law enforcement perspective it argues more sophisticated ICT is needed to facilitate information sharing and analysis, whatever organisational structure is implemented (i.e. local, federal, national). It deepens the understanding of practical, systemic barriers to effective ICT use within intelligence systems, exposing the nature of discretion in nuanced practitioner behaviour. The research also reveals the significant challenge all law enforcement agencies face in transforming their current approach, and explores their appetite to use ICT more ambitiously in cross-border interoperability.

This study seeks to scrutinise law enforcement practice in more detail. It will examine operational practice across three countries to establish whether there is consistency in the way information management is conducted and whether it is being used to its full potential. If there are consistent international patterns at an operational level, this should provide a better indication as to how to improve effectiveness and efficiency.

## METHODOLOGY

This study is part of a larger review examining law enforcement information sharing. To explore the nuances involved in the use of ICT, a qualitative approach was favoured

(Sarantakos, 2005). It uses semi structured interview data from UK, Australia and New Zealand. Participants were recruited using purposive (i.e. participants were selected intentionally based on having relevant experience) and snowball (i.e. participants were asked to recommend other practitioners who had experience in this area) sampling techniques; every invited individual agreed to take part. All participants (n=62) had experience in intelligence and in the investigation of SOC, and all agencies use digital information systems. Most participants were aligned with UK based police forces including regional, national and international units (i.e. West Midlands Regional Organised Crime Unit, Merseyside Police, International Crime Coordination Centre [ICCC], Europol, National Police Chiefs' Council [NPCC]) (n=28), non-governmental organisations (NGOs) or the commercial sector (i.e. animal welfare groups, an international technology company, and the Federation Against Copyright Theft [FACT]) (n=7), and wider law enforcement agencies, such as Border Force, Trading Standards, and HM Revenue and Customs (HMRC) (n=6). The representatives ranged between senior managers to practitioners. The remaining participants comprised a range of senior and middle managers, operatives and analysts from the Australian Federal Police (AFP), Victoria Police, Australian Institute of Criminology (AIC), ACIC, South Australia Police and New Zealand Police (n=16). Staff from the Australia New Zealand Policing Advisory Agency (ANZPAA) and a senior University academic (n=5) were also interviewed.

The three countries were chosen as they provide an interesting cross-national comparison. All are English-speaking and operate within similar legal frameworks. However, in terms of organisational structure, whilst the UK is primarily policed through local jurisdictions, Australia adopts a state and territory-based model, and New Zealand experiences a national police force. While law enforcement practices and ICT infrastructures vary not only between countries but also across regions and agencies, this diversity enriches the study's insights into information management and the use of ICT. Moreover, the inclusion of practitioners from both operational and strategic levels, across a range of roles, agencies, and levels of ICT expertise, captures a more comprehensive perspective on the associated challenges and opportunities.

The interviews predominantly took place on an individual face-to-face basis, albeit a small number of interviews were conducted via Microsoft Teams and/or involved more than one participant. The questions were designed to explore two topics: the threat posed by organised crime and how law enforcement practitioners use ICT to share information when tackling SOC. The study followed appropriate ethical procedures, and all respondents provided consent to take part (Punch, 1986). Interviews were audio recorded and transcribed verbatim before undergoing thematic analysis, manually (i.e. reading, annotating, coding and organising the data by hand), to highlight reoccurring topics, which were collapsed into themes (Braun & Clarke, 2006, 2021). This was done separately by researchers who then collectively examined their findings and agreed the final themes.

## RESULTS

Four main themes emerged from the interviews and are detailed below:

*i) An increasing threat*

All practitioners from all three countries verified government and academic accounts, which argued the harm associated with SOC had escalated in volume and diversity, and become more transnational. The following quotes are indicative of this consensus:

> "*Most of the jobs that we investigate, there has to be some overseas element in them….slavery and trafficking…drug trafficking…firearms offences….So as a consequence, I think our life becomes a bit more difficult and theirs [offenders] probably becomes a bit more easier*" (P10).

> "*Around 12% of our arrests are foreign nationals… but about 30% of our membership of our [organised crime] map are foreign nationals, now that's an indicator. What we are saying is we are seeing that OCGs [Organised Crime Groups] are specifically targeting people from other countries. Because basically, if I now bring in someone from Chile as part of my OCG then guess what? I've got a whole new marketplace, you know it's like having area managers from different locations… So, crime has always been international, but I think it's increasingly international*" (P12).

> "*Major OC [organised crime] entities routinely travel to facilitate crime and to avoid arrest*" (P61).

Participants pointed out the threat came from all continents and not just neighbouring countries. They explained global markets had been exploited by offenders through technology, especially encrypted communication. As one participant explained:

> "*If you can use the internet, you understand the dark web, TOR [The Onion Router] networks, you can get yourself an onion browser… you can buy yourself stuff and you can start pumping it out…… one was making £10,000 [UK] a week just on one of the criminal commodities [illegal lab sourced drugs imported from India*]" (P3).

As representatives from all three countries had witnessed an increased threat, facilitated by technology, the next theme explored their response.

*ii) The law enforcement use of ICT in combatting SOC*

There was a strong consensus, from all participants, that ICT benefits them. Numerous examples were provided as to the assistance it provided in finding offenders already wanted:

> "*So we will use all the usual systems that we have access to: police systems, public access systems, information from private companies via DPAs [data processing agreement] and… [provides confidential example]. There's… carriers, air carriers, so*

*like your airlines, bus companies, ferries, travel companies… its information sharing about what people are buying, what IP addresses they are using, telephone numbers, who they are flying with… this has great benefits for us and then you put it together and then you get location, get your footprint and we move onto the next stage which is boots on the ground stuff*" (P11).

Most practitioners provided examples whereby ICT was used proactively to identify, investigate and disrupt offenders. One example focused on a vast network of Romanian-affiliated OCGs, active in the UK, Europe and the USA:

"*So, using green notices and Europol notices and emailing different agencies around the world, these people would stop being able to travel really quickly and it would force them to use illegal means at great expense. At a stroke, one person with a spreadsheet could stop 1500 people being able to travel legally around the entire world*" (P28).

Automatic Number Plate Recognition (ANPR) was another regularly used tactic, especially in disrupting offenders by continually seizing undocumented vehicles, purchased using criminal assets. The next theme explored whether the potential for the use of ICT could be increased.

*iii) Maximising potential: identifying the current challenges associated with information management*

Despite the use of ICT in proactive investigations, there was a shared and resounding view that more could be done to realise its potential. Again, this finding was replicated across the three countries. As P2 explained,

"*So, whether its automatic number plate recognition or data from mobile phone telephony work, or crime information systems. I mean, you know that if you put good data scientists over all that information, you'd get some brilliant patterns… we don't do that*".

Several reasons were provided for not exploiting this potential. Whilst most participants highlighted resources, this was particularly emphasised by UK participants. The following quotes explain the context:

"*The funding is never sufficient to be able to do what you want to do… Every crime now is committed with computers ….., even mobile phones. You know every crime has that element and the police technologically are always playing catch up… but now with technology, it's fallen further behind because they don't have the resources*" (P1).

"*If there's a list [for conducting information checks] and they can only do something like 300 a month. So, if you're 301, you're going to wait till the next month*" (P2).

"*We are actually overwhelmed… Because, yeah, we're drowning in data without the tools to exploit it*" (P3).

However, the more common concern found across all countries was the inability to operate across borders, and the difficulty in connecting disparate systems, to facilitate a more complete intelligence picture. This was an issue no matter what the organisational structure of the agency was. For example even in a national structure (NZ) practitioners needed to share information with other agencies involved in policing. As participants explained:

> "*The system and software incompatibility is a big thing and having loads of systems and working in silos*" (P7).
>
> "*We're not anywhere near joined up as we'd like to think we are from a domestic [or] international point of view*" (P10).
>
> "*Every system equals more work and more dysfunction*" (P49).

These issues appeared exacerbated by the local practice and procedures involved across different jurisdictions. Participants highlighted that there was no common process, with levels of co-operation influenced by specific agencies and their staff. This generated considerable bureaucracy as, for example, a Memorandum of Understanding could take "*up to six months*" (P5) due to the involvement of local legal departments. There was also considerable difference across jurisdictions with information access, processing time, data quality, and the outputs produced:

> "*you've got lots of organisations that have their own remits and responsibilities so there isn't effective enforcement of national standards [of information management]*" (P22).
>
> "*for example, [two Australian territories identified], we use the [system name omitted] quite differently …., and that presents challenges when you try to, for example, create one domestic violence report that everyone uses because everyone's got their own different flavour*" (P57).

The necessity to type information into multiple systems, or "double keying" (P21), also impacted upon efficiency and data quality (P22). Overall data accuracy was a concern, with one participant summarising this as "shit in, shit out" (P48):

> "*we've got masses of historic records that's never been cleansed and never been checked……I actually did a search…and there was thousands of Mickey Mouse's, Donald Duck, Goofy, the list was endless… the records haven't been corrected*" (P21).

Human factors were consistently mentioned. Several participants had experienced receiving a poorer service due to personnel changes in partner agencies. In contrast, many participants cited how helpful partner representatives could be when providing contextual insight. Local knowledge could assist in identifying fictitious names, which saved considerable time. Issues like this seemed to be behind the importance that practitioners placed in forging human relationships:

> "*We ask for stuff, and it doesn't come… [we ask a contact in that country] can you help push it along. They'll help push it along then the next day you've got rafts of information. So that really helps having that human touch, that point of contact. Intelligence gathering, it's no good if there's no point of contact – to just send it off in the ether – where does it go? It's not done, is it?*" (P11).

Practitioners also highlighted offenders exploited these constraints. For example, offenders realised isolated acquisitive crime, even if "*high value*" (P28), would not be a priority for law enforcement. Therefore, by travelling anonymously between different countries, they could engage in high value jewellery theft with little chance of detection.

*iv) The ambition to increase the use of technology in information management*

As technology continues to evolve, this provides increased opportunities for law enforcement in the analysis of information. However, as the preceding comments illustrate, the current information management process appears to rely heavily on human discretion and a "*mindset of cooperation*" (P51). As such, this final theme explores practitioner appetite for greater automation in information analysis, both to connect and interrogate systems. Most participants recognised the benefits greater access and analytical power could bring:

> "*Oh they'll come back [the organisation who holds the dataset] and say there's 50 results. We can't narrow that down. But if you're looking yourself… it opens up so much more. [It would be useful] to be able to have direct access to it*" (P2).
>
> "*Personally, I think [direct access to databases from other agencies] is a good thing. The number of times we are asking for stuff, and we are waiting and waiting and waiting, and then two weeks later, sending more emails asking again. It can be a really slow process*" (P13).

Indeed, some participants wanted automation to go much further in connecting datasets. An interesting perspective came from P35:

> "*I think PND [UK Police National Database] as a tool is really good. It's certainly the best thing we've got, and it may be the best thing internationally. But I still think that PND is rooted in 20th Century police thinking, not 21st Century police thinking. Because back in the late 80s early 90s when we were police officers, you could solve everything with police information. But now it's probably 30% of what you need. And if you look at [mentions private commercial company]… they will have PND on their system, PNC [UK Police National Computer] on their system, they will pull in all the information from the City of London, all the organised crime and money laundering entities, they'll pull in all the Equifax stuff, they will have the passport database, they will have the land registry, they all do open source, they will do social media, all on the same platform. That is 21st Century thinking to me, not just police data, it is how that data then cross references with all the data – whether its [national car parking company] or whatever, that's where the real value of it lies, I think*" (P35).

The potential of AI was also mentioned in terms of its potential to assist with data analysis and direct police activity:

> "*we've got this project… trying to combine risk databases for domestic violence… they've got some AI models that can go through instant reports and extract keywords. So you can look at, you know, 'strangulisation', 'jealousy'… and everything's got a flag. You've got a flag for spitting, a flag from mental health concern, a flag from false allegations, a flag for possible use of weapons… it means that when you're sending people to all these different jobs, it's difficult to know what's the one that's really concerning and what you've got to really pay attention to, so we're trying to automate this algorithm*" (P43)

However, practitioners also voiced concerns as to how this could occur in practice. Some declared ethical concerns in sharing information on suspects who were not convicted, as well as reticence in sharing information from specific sources (P11). There was uneasiness about too much information simply becoming "white noise", acting as a distraction (P12). Many underlined the importance of establishing protocols to direct the type and circumstances of information sharing, including the expected actions from the recipient (P12). Practitioners were also concerned about risk, in terms of who could access different levels of information. Yet, some participants argued technology could be used to control access and maintain an audit trail:

> "*we should be able to interrogate each of those databases. We're all doing the same job, from the policing point of view. We should all have the correct security clearance and corruption elements aside of that, there should be trust in agencies to be able to do that… being able to do it electronically by the use of APIs is the right way to do it because you've got the audit trail of what's happening*" (P21).
>
> "*our [Australian state] intel branch can put a layer of ACL [Access Control Lists] over the top…. people should know that something exists but not necessarily see what it is... when you look at a person, you can see that they've got 30 occurrences and you can only see 28 of those..., but you at least know that they exist*" (P57).

Whilst representatives from the UK (local jurisdictions) and Australia (state/territorial jurisdictions) often cited the "*need for one system all [agencies] can communicate on*" (P45), representatives from New Zealand (national system) also experienced challenges. This was because not all information was on one system and the police relied heavily on other organisations to provide information, especially involving transnational offenders. Further, the difficulties associated with the collection, analysis and dissemination of information continued to be present, even with national systems.

## DISCUSSION

21st Century technology has played an important role in building an interdependent, information rich society, which has transformed the way in which citizens live, work, and communicate (Deloitte, 2018; Schwab, 2015). Innovation in ICT, specifically digitisation and the internet, has been difficult to regulate and has brought an unintended consequence in terms of transnational SOC. In adapting to this challenge law enforcement agencies rely on intelligence-led approaches (Ratcliffe, 2016). These require effective and efficient information collection, analysis, and dissemination of pertinent and timely data to target prolific offenders and reduce the vulnerability of victims and locations. Sadly, information management practices are often criticised, with intelligence failures described as inevitable (Wirtz, 2023). Previous responses to these intelligence failures have often followed similar paradigms using extra resources, which are often piecemeal and sub-optimal. For example, Europol and US-based fusion centres are one example where representatives from diverse jurisdictions come together to share information. However, the practitioner remains in control of their own information and decides what will or will not be shared (Phythian et al., 2024). Further, USA fusion centres are estimated to cost over $330m per annum and are criticised for not providing value for money (Farivar, 2021; McQuade, 2019; Wardlaw, 2015). Similarly, systems that primarily rely on human input are slower to operate, are constrained in terms of the data they handle, and are more prone to individual error. This study wanted to explore this issue from a fresh perspective to provide new insight and opportunities for change. Specifically, it examines whether law enforcement agencies are harnessing the potential of ICT to tackle SOC.

Whilst the law enforcement experts involved in this study were based in three countries, their views showed considerable consensus. The study obtained tangible examples of how the SOC threat had increased in their jurisdiction. Further, practitioners illustrated expert knowledge of the 'information rich environment' within which they operated. Indeed, most participants – at an individual level - provided examples of how data was used to either arrest or disrupt active transnational OCG members. However ultimately, they felt that whilst the potential exists to revolutionise intelligence led methods, this capability was not being realised.

Whilst the technology exists to improve information management through connecting databases and enhancing automation, this has been slow to develop in law enforcement. Even in areas where this has developed (e.g. the UK PND) the system is underutilised with some practitioners commenting negatively on its useability (Phythian and Kirby, 2022). In Australia, the state / territory law enforcement structure has also tried to accommodate cross boundary information sharing. The government has recently established the NCIS system, which connects specific law enforcement information systems across a small number of agencies (ACIC, 2023). However, none of the participants in this study were able to provide examples as to how this has been used in practice. A participant in New Zealand explained having a national structure makes information exchange faster and easier.

However, information sources are still maintained in various systems, and other relevant information is held within partner databases. Therefore, even in a national agency, an all-encompassing database remains elusive.

The lag in embracing technological solutions, and the preference of law enforcement to utilise human intensive systems is best explained through a series of connected challenges. At the outset it should be recognised that managing information is a complex business, which starts by searching and collating relevant information. However, this can be difficult to find as offenders disguise their identity and behaviour, and the data itself is separated into different forms (audio, video and text), and held across separate agencies and jurisdictions. Once found, effective systems and analytical tools need to be in place to establish its relevance, for example identifying the criminal links between people, places and actions. Finally, systems must be able to disseminate the intelligence, in a timely and appropriate manner, to those who can use it. Law enforcement agencies, who were originally designed to provide local services, are poorly equipped in responding to national and international trends.

In terms of solutions, for those who support increased amalgamation of forces with the ultimate goal of a national structure (UK Parliament, 2013), this would still require the rationalisation of legacy systems and the cooperation of those external to the police. Cross border cooperation is complicated due to legislation and protocols, which dictate how different jurisdictions share and use information. Participants in this study bemoaned the effort required when sharing information across borders, with each jurisdiction requiring its own tailored approach. The case of Barzan Majeed, convicted for 121 counts of people smuggling, epitomises this. Although sought by UK and Belgium law enforcement agencies, he was found by journalists. The Belgian public prosecutor said, “For journalists, it’s easier to track him down because there is no formal procedure they have to follow…..they [BBC Journalists] moved from one source to another, from one city to another, from one country to another, in a way that police prosecutors can’t” (Mitchell, 2024).

Finally, an underreported element in terms of this problem is police organisational culture. This topic shows enduring features over its 50 years of research (Banton, 1964), including officers favouring ‘real police work (arrests)’, an inclination towards risk aversion, and valuing the familiar (Loftus, 2009). These, together with other attributes, may help explain officer discretion when deciding to share or withhold information, and clarify why human relationships are nurtured to facilitate cooperation. Also, when compared to the private sector, law enforcement agencies are said to demonstrate a paucity of evaluation. This is because, as the only available service provider in their field, they continue to be used even when providing a poor service (Seddon, 2008). Further, Syed (2015) argues public sector organisations (including law enforcement), operate closed loop systems where they do not recognise failure as a learning opportunity, but as something to disguise and defend. This

makes law enforcement agencies more interested in the activity they conduct (the output), rather than the outcome achieved (Shane, 2010). None of these cultural characteristics are suited to the promotion of technological innovation.

To overcome all these interconnected challenges requires strong strategic leadership. To rationalise and connect systems, implement and automate analytical tools, and persuade practitioners to change working practice requires high level co-operation, regulation and resources. During this study, whilst lots of good will and effort was displayed, there were few examples of information management being valued at a strategic level and no consistent vision in terms of how systems should work. Although invited, no practitioner could provide evidence to show information sharing was prioritised at an organisational level, nor provide any evaluation of system effectiveness and efficiency. This leaves practitioners within individual agencies doing the best they can to improve their part of business, however such action can be piecemeal and fail to embrace the potential.

## Research limitations

This study offers valuable insights through its in-depth, cross-national qualitative design, involving 62 experienced law enforcement professionals from the UK, Australia, and New Zealand. The diversity of roles - spanning operational, tactical, and strategic levels - across a wide range of agencies and sectors enriches the data and enhances the practical relevance of the findings. Thematic analysis of semi-structured interviews provides a nuanced understanding of ICT use in tackling SOC. However, there are several limitations that merit consideration. The reliance on purposive and snowball sampling may introduce bias, as participants were selected through existing professional networks, potentially limiting the diversity of viewpoints. Although the international scope is a strength, the sample is unevenly distributed, with a predominance of UK-based participants and limited representation from some agencies, potentially skewing the cross-jurisdictional insights. A more balanced and systematic sampling strategy could strengthen generalisability and allow for clearer comparisons across countries, agencies, and professional levels. Furthermore, the study did not explicitly quantify variables such as frequency of ICT use or extent of relevant expertise (i.e. with ICT or SOC), which could limit analytical precision and the potential for comparison across subgroups. Finally, while a qualitative approach is well-suited to exploring complex real-world experiences, it also introduces subjectivity and may be influenced by individual expertise and focus. However, this limitation was mitigated by an inter-rater approach and the relevant professional experience of one of the researchers, enhancing the credibility and consistency of the findings.

## Conclusion

Technology has undoubtedly transformed society. However, an unintended consequence has been the increase in organised crime. Whilst ICT has improved the effectiveness and efficiency of law enforcement, much more can be achieved. System architects have already

displayed their ability to connect and control access to disparate systems using technological pipelines. Further, the private sector has shown how technology, together with data scientists, can increase the speed and scale of information analysis and management. This study has outlined several interconnected reasons to explain why this potential is not being realised, including legacy systems, local protocols and organisational culture. In an age where data continues to increase exponentially, it appears only a matter of time before law enforcement agencies are forced to embrace more technological innovation. This could significantly improve efficiency and reduce the negative consequences of practitioner discretion. However, it should also be recognised that several expert practitioners in this study voiced implementation concerns. Konaev and Chasal (2021) identify the importance of 'machine trust', which explains the level of confidence in the technology to deliver appropriate and accurate results. If findings are accepted without question, then too much trust can be dangerous and conversely too little trust can result in technology being ignored. In a period when behavioural analytics and AI is moving forward at pace, the process in which the machine finds its answer must be transparent (Babuta *et al.*, 2020). This study shows considerable effort at a strategic level is needed to improve information sharing with delays exploited by SOC offenders, who display no reticence in embracing technology.

## REFERENCES


Australian Criminal Intelligence Commission (ACIC) (2017), "Organised crime in Australia 2017", available at: https://www.acic.gov.au/sites/default/files/2020-08/oca_2017_230817_1830.pdf (accessed 22 April 2024).

Australian Criminal Intelligence Commission (ACIC) (2021), "Chair annual report", available at: https://www.acic.gov.au/sites/default/files/2022-11/2020-21_acic_chair_annual_report_internals_v14_digital.pdf (accessed 22 April 2024).

Australian Criminal Intelligence Commission (ACIC) (2023), "Expanding the capabilities of the National Criminal Intelligence System", available at https://www.transparency.gov.au/publications/attorney-general-s/australian-criminal-intelligence-commission/australian-criminal-intelligence-commission-annual-report-2022-23/section-3%3A-management-and-accountability/feature%3A-expanding-the-capabilities-of-the-national-criminal-intelligence-system (accessed 17 April 2024).

Babuta, A., Oswald, M. and Janjeva, A. (2020), "Artificial intelligence and UK national security: policy considerations", available at https://static.rusi.org/ai-national-security-final-web-version.pdf (accessed 26 April 2024).

Banton, M. (1964), *The Policeman in the Community*, Tavis, London.

Barker, C. (2019), "Transnational, serious and organised crime", available at https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/BriefingBook46p/OrganisedCrime (accessed 20 April 2024).

Bartley, K. (2023), "Big data statistics: how much data is there in the world", available at: https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/ (accessed 10 April 2023).

Beccaria, C. (1986 [1764]), *An Essay on Crimes and Punishments,* Hackett Publishing Company Inc., Indianapolis.

Beckford, M. (2018), "One in five people arrested in Britain are foreign: Crime tourism spikes as police figures reveal an overseas suspect is seized every three minutes", *Daily Mail*, 18 August, available at: https://www.dailymail.co.uk/news/article-6074691/One-five-people-arrested-Britain-foreign-one-three-minutes.html (accessed 10 April 2023).

Bellingcat (2018), "Skripal suspects confirmed as GRU operatives: Prior European operations disclosed", 20 September, available at: https://www.bellingcat.com/news/uk-and-europe/2018/09/20/skripal-suspects-confirmed-gru-operatives-prior-european-operations-disclosed/ (accessed 16 June 2024).

Birdi, K., Griffiths, K., Turgoose, C., Alsina, V., Andrei, D., Băban, A., Bayerl, P.S., Bisogni, F., Chirică, S., Costanzo, P., Fernández, C., Ficet, J., Gascó, M., Gruschinske, M., Horton, K., Jacobs, G., Jochoms, T., Krstevska, K., Mirceva, S., Mouhanna, C., van den Oord, A., Oțoiu, C., Rajkovcevski, R., Rațiu, L., Reguli, Z., Rus, C., Stein-Müller, S., Stojanovski, T., Vallet, N., Varga, M., Vít, M. And Vonaș, G. (2020), "Factors influencing cross-border knowledge sharing by police organisations: an integration of ten European case studies", *Police Practice and Research*, Vol. 22 No. 1, pp. 3-22. DOI: 10.1080/15614263.2020.1789462

Birkinshaw, J. (2014), "Beyond the information age", available at: https://www.criticaleye.com/inspiring/insights-detail-new.cfm?id=3996 (accessed 14 March 2023).

Bradford, B., Yesberg, J.A., Jackson, J. and Dawson, P. (2018), "Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology", *The British Journal of Criminology*, Vol. 60 No. 6, pp.1502–1522. DOI: 10.1093/bjc/azaa032

Brantingham, P.J. and Brantingham, P.L. (1984), *Patterns in Crime*, MacMillan, New York.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp.77–101. DOI: 10.1191/1478088706qp063oa

Braun, V. and Clarke, V. (2021), *Thematic Analysis: A Practical Guide*, Sage, London.

Broeders, A.P.A. (2007), "Principles of forensic identification science", Newburn, T., Williamson, T., and Wright, A. (Ed.s), *Handbook of Criminal Investigation*, Willan, Cullompton, pp.303-337. DOI: 10.4324/9780203118177

Canter, D. and Gregory, A. (1994), "Identifying the residential location of serial rapists", *Journal of the Forensic Science Society*, Vol. 34, pp.169-175. DOI: 10.1016/S0015-7368(94)72910-8

Carter, J.G. (2015), "Inter-organizational relationships and law enforcement information sharing post 11 September 2001", *Journal of Crime and Justice,* Vol. 38 No.4, pp.522-542. DOI: 10.1080/0735648X.2014.927786

Carter, J.G., Carter, D.L., Chermak, S., and McGarrell, E. (2016), "Law enforcement fusion centers. Cultivating an information sharing environment while safeguarding privacy", *Journal of Police and Criminal Psychology*, Vol. 32, pp.11–27. DOI: 10.1007/s11896-016-9199-4

Chiricos, T.G. and Waldo, G.P. (1970), "Punishment and crime: an examination of some empirical evidence", *Social Problems*, Vol. 18, pp.200-217. DOI: 10.1525/sp.1970.18.2.03a00070

Cornish, D. and Clarke, R.V. (1986), *The Reasoning Criminal: Rational Choice Perspectives on Offending*, Springer-Verlag, Hague.

Deloitte (2018), "Policing 4.0: Deciding the future of policing in the UK", available at: https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/PublicSector/deloitte-uk-future-of-policing.pdf (accessed 18 March 2023).

Europol (2017), "European union serious and organised crime threat assessment, crime in the age of technology", available at: https://www.europol.europa.eu/cms/sites/default/files/documents/report_socta2017_1.pdf (accessed 20 April 2024).

Europol (2021), "European Union serious and organised crime threat assessment, a corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime", available at: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf (accessed 20 April 2024).

Farrell, G. and Tilley, N. (2017), "Technology for crime and crime prevention: a supply side analysis", Leclerc, B. and Savona, E.U. (Ed.s), *Crime Prevention in the 21st Century: Insightful approaches for crime prevention initiatives,* Springer International Publishing, Cham, Switzerland, pp. 377-388.

Farivar, C. (2021), "20 years after 9/11, 'fusion centers' have done little to combat terrorism", *NBC News,* 11 September, available at: https://www.nbcnews.com/business/business-news/20-years-after-9-11-fusion-centers-have-done-little-n1278949 (accessed 12 March 2025).

Ferguson, A.G. (2017), "*The rise of big data policing: surveillance, race and the future of law enforcement"*, New York Press, New York.

Fielding, N. (2002), "Cop canteen culture", Newburn, T. and Stanko, E. (Ed.s.), *Just boys doing business*, Routledge, London, pp.46-63.

Gerencer, T. (2020), "The top 10 worst computer viruses in history", available at: https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history (accessed 16 June 2024).

Gibbs, J.P. (1968), "Crime, punishment and deterrence: another analysis of Gibbs' data", *Science Quarterly*, Vol. 48 No. 4, pp.515-530.

Global Initiative Against Transnational Organized Crime (2023), "The Organized Crime Index 2023", available at https://globalinitiative.net/analysis/ocindex-2023/ (accessed 25 June 2024).

Gottschalk, P. (2009), *Entrepreneurship and Organised Crime: Entrepreneurs in illegal business*, Edward Elgar Publishing Ltd, Cheltenham.

Haenlein, C. and The Lord Evans of Weardale KCB DL (2023), "A boundless threat? The rise of organised crime in the UK", available at https://www.rusi.org/explore-our-research/publications/commentary/boundless-threat-rise-organised-crime-uk (accessed 20 April 2024).

Harris, A., Eleanor, S., Bradford, E. and Janjeva, A. (2023), "Behavioural analytics and UK national security", available at: https://cetas.turing.ac.uk/sites/default/files/2023-03/cetas_research_report_-_behavioural_analytics_and_uk_national_security_1.pdf (accessed 16 June 2024).

Kirby, S. and Turner, G. (2007), "The use of ANPR in major crime investigation", *Journal of Homicide and Major Incident Investigation*, Vol. 3 No. 2, pp.35-42.

Konaev, M. and Chahal, H. (2021), "Building trust in human-machine teams," *Brookings*, 18 February, available at: https://www.brookings.edu/techstream/building-trust-in-human-machine-teams (accessed 24 April 2024).

Lück, D., Limmer, R. and Bonß, W. (2006), "Theoretical approaches to job mobility", Widner, E. and Schneider, N.F. (Ed.s), *State-of-the-art of mobility research. A literature analysis for eight countries*, Job Mobilities Working Paper No. 2006-01, pp.5–39.

Loftus, B. (2009), *Police Culture in a Changing World*, Oxford University Press, Oxford.

McQuade, B. (2019), *Pacifying the homeland: Intelligence fusion and mass supervision*, University of California Press, California.

Mitchell, S. (2024), "Why the BBC could track down a people smuggling kingpin before the police", *BBC*, 18th May, available at: https://www.bbc.co.uk/news/articles/c2qv0grgy7yo.

Napoleon, P., Saturnia, O., Shoesmith, M. and Petrovitch, J. (2021), "The use of encrypted communications by criminals", available at: https://www.counterterrorismgroup.com/post/the-use-of-encrypted-communications-by-criminals (accessed 16 June 2024).

Niels, G. (2023), "AI and predictive analytics in national security: Navigating unchartered waters", available at: https://www.linkedin.com/pulse/ai-predictive-analytics-national-security-navigating-niels-groeneveld (accessed 16 June 2024).

Nuth, M.S. (2008), "Taking advantage of new technologies: for and against crime", *Computer Law and Security Review*, Vol. 24 (5), pp.437-446. DOI: 10.1016/j.clsr.2008.07.003

Office of National Statistics (ONS) (2021), "Internet sales as a total of retail sales", available at: https://www.ons.gov.uk/businessindustryandtrade/retailindustry/timeseries/j4mc/drsi (accessed 22 June 2021).

Phythian, R. and Kirby, S. (2022), "What does the UK Police National Database tell us about the future of police intelligence?", *Policing: A Journal of Policy and Practice*, Vol. 17. DOI: 10.1093/police/paac074

Phythian, R., Kirby, S. and Swan-Keig, L. (2024), "Understanding how law enforcement agencies share information in an intelligence-led environment: how operational context influences different approaches", *Policing: An International Journal*, Vol. 47 No. 1, pp. 112-125. DOI: 10.1108/PIJPSM-06-2023-0073

Punch, M. (1986), *The politics and ethics of fieldwork*, Sage, Beverly Hills.

Ratcliffe, J. (2016), *Intelligence-led Policing,* Routledge, Abingdon.

Rossmo, D.K. (2000), *Geographic Profiling,* CRC Press, Boca Raton, FL.

Sarantakos, S. (2005), *Social Research* (3rd ed), Palgrave Macmillan, Hampshire.

Schwab, K. (2015), "The fourth industrial revolution: what it means and how to respond", available at: https://www.foreignaffairs.com/world/fourth-industrial-revolution (accessed 2 April 2023).

Seddon, J. (2008), *Systems thinking in the Public Sector*, Triarchy Press, Axminster.

Shane. J.M. (2010), "Performance management in police agencies: a conceptual framework", *Policing: An International Journal of Police Strategies and Management*, Vol. 33 No. 1, pp.6-29. DOI: 10.1108/13639511011020575

Sherman, L. W. (1995), "Hot spots of crime and criminal careers of places", Eck, J.E. and Weisburd, D. (Ed.s), *Crime and place: Crime Prevention Studies* (vol. 4), Criminal Justice Press, Monsey, NY, pp.35-52.

Song, C., Qu, Z., Blumm, N. and Barabási, A-L. (2010), "Limits of predictability in human mobility", *Science*, Vol. 327 No. 5968, pp.1018–1021. DOI: 10.1126/science.1177170

Syed, M. (2015), *Black Box Thinking: The Surprising Truth about Success (and why some people never learn from their mistakes)*, John Murray Publishers, London.

Taylor, R. and Russell, A. (2012), "The failure of police fusion centers and the concept of a national intelligence sharing plan", *Police Practice and Research: An International Journal*, Vol. 13 No. 2, pp. 184-200. DOI: 10.1080/15614263.2011.581448

Tyler, T.R. (2006), *Why people obey the law*, Princeton University Press, Princeton.

UK Parliament (2013), "Police: independent police commission report", available at https://hansard.parliament.uk/lords/2013-12-05/debates/13120564000842/PoliceIndependentPoliceCommissionReport (accessed 13 March 2025).

Wardlaw, G. (2015), "Is the Intelligence Community Changing Appropriately to Meet the Challenges of the New Security Environment?", available at: http://press-files.anu.edu.au/downloads/press/p319221/pdf/ch082.pdf (accessed 19 March 2023).

Weisburd, D. (2015), "The Law of Crime Concentration and the Criminology of Place", *Criminology*, Vol. 53 No. 2, pp.133-157. DOI: 10.1111/1745-9125.12070

Wirtz, J.J. (2023), Are intelligence failures still inevitable? *International Journal of Intelligence and Counter Intelligence,* Vol. 37 No. 1, pp.307-330. DOI: 10.1080/08850607.2023.2214328

Zhang, W., Shen, Q., Teso, S., Lepri, B., Passerini, A., Bison, I. and Giunchiglia, F. (2021), "Putting human behaviour predictability in context", *EPJ Data Science,* Vol. 10 (Article 420), available at https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-021-00299-2#citeas (accessed 14 March 2025).

# Does Information Communication Technology facilitate or solve crime? Exploring the experience of law enforcement practitioners in three countries.

**Authors names and affiliations**

Prof Stuart Kirby, SKirby3@uclan.ac.uk, School of Law and Policing, University of Central Lancashire, UK.

Orcid ID: https://orcid.org/0000-0002-3049-1248

Dr Rebecca Phythian[1], PhythiaR@edgehill.ac.uk, School of Law and Criminal Justice, Edge Hill University, UK.

Orcid ID: https://orcid.org/0000-0001-6423-2116 | X: @beckyphythian | LinkedIn: https://www.linkedin.com/in/rphythian/

**Author biographies**

Professor Stuart Kirby is an Emeritus Professor in Policing and Criminal Investigation. He previously served as a Detective Chief Superintendent at Lancashire Constabulary (UK) with responsibilities including Intelligence, Major Crime, Organised Crime and Counter Terrorism.

Dr Rebecca Phythian is a Reader in Policing and a UK Research and Innovation Future Leaders Fellow. Her research explores international law enforcement information exchange.

**Keywords**

information communication technology (ICT), technology, information sharing, information exchange, intelligence, law enforcement, multi-agency, serious organised crime (SOC)

**Acknowledgements**

The authors would like to thank all those who participated in this research. They also extend their thanks to Lauren Swan-Keig for her assistance during the UK data collection stage, and to Cristina Silvestri and Nicole Fischhaber for transcribing interviews.

**Funding statement**

This work was supported by a UK Research and Innovation Future Leaders Fellowship under Grant MR/V027344/1.

The authors report there are no competing interests to declare.

[1] Corresponding author