



University of New South Wales Law Research Series

Datafication and the Practice of Intelligence Production

**Janet Chan, Carrie Sanders, Lyria Bennett Moses and Holly
Blackmore**

[2022] *UNSWLRS* 10
(2022) *Big Data & Society*

UNSW Law
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au

W: <http://www.law.unsw.edu.au/research/faculty-publications>

AustLII: <http://www.austlii.edu.au/au/journals/UNSWLRS/>

SSRN: <http://www.ssrn.com/link/UNSW-LEG.html>

Datafication and the practice of intelligence production

Big Data & Society
January–June: 1–13
© The Author(s) 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20539517221089310
journals.sagepub.com/home/bds



Janet Chan¹, Carrie Sanders² , Lyria Bennett Moses¹ 
and Holly Blackmore¹ 

Abstract

Datafication of social life affects what society regards as knowledge. Jasanoff's regimes of sight framework provides three ideal-type models of authorised knowing in environmental data practice. This paper applies Jasanoff's framework for analysing intelligence practice through an exploratory empirical study of crime and intelligence practitioners in a selection of police services in Australia, New Zealand, Canada and the United States. The paper argues that the 'view from somewhere' (VFS) captures the essence of existing police intelligence practices in the four countries but the 'view from nowhere' (VFN) is emerging as a possible future for police intelligence – an approach promoted by technology companies and supported mainly by police leaders and managers. The paper investigates the challenges and limits of a shift by police from VFS to VFN in the production of intelligence; the challenges are primarily political, which threaten the dominance of police contextual knowledge over 'scientific' knowledge. These political challenges also have symbolic and material implications. The paper concludes that, because of these challenges, a complete shift from VFS to VFN is not likely to happen. At best the two models might co-exist with the latter subordinate to the imperatives of the former, resulting in further tension between sworn officers and civilians, organisational inertia, as well as technologies that may be under-utilised or abandoned.

Keywords

Datafication, material barriers, symbolic barriers, qualitative research, police intelligence, regimes of sight

Introduction

Advances in information technology (IT) have transformed social relations through the ubiquity and connectivity of digital sensors and communication networks (Smith et al., 2017). Many aspects of social life have undergone rapid 'datafication', that is, social phenomena are put 'in a quantified format so that [they] can be ... analyzed' (Mayer-Schönberger and Cukier, 2013: 78). The criminal justice system is not immune to this process (Dencik, 2019; Ferguson, 2017). While street policing and criminal investigation still capture the public imagination, this occurs alongside the work of criminal intelligence analysts who must collect and analyse data in response to changing crime conditions and do 'sensemaking' to define what is important in order to make actionable recommendations (NASEM, 2019).

There is a growing body of research on criminal intelligence analysis. One focus has been on the increased reliance on data, such as in hot spot mapping wherein retrospective data is used to identify high concentrations of crime in order to identify where to focus police and

crime reduction strategies (Chainey et al., 2008) and social network analysis which seeks to identify patterns in social structures in order to relate those structures to the overall functioning of a criminal network (Bright and Whelan, 2020; Burcher, 2020), as well as the impact analytic practices have on the effectiveness of crime control (Ratcliffe, 2010).

In this paper, we focus on how datafication may have affected what forms of intelligence production are valued in Western democratic states and identify barriers to change from one approach to another. We apply Sheila Jasanoff's (2017) 'regimes of sight' framework and the

¹Faculty of Law & Justice, The University of New South Wales, Sydney, Australia

²Department of Criminology, Wilfrid Laurier University, Brantford, Ontario, Canada

Corresponding author:

Carrie Sanders, Department of Criminology, Wilfrid Laurier University, 20 Charlotte Street, Brantford, Ontario, Canada.
Email: csanders@wlu.ca



literature on police use of technology to conceptualise the political, symbolic and material implications of two competing narratives on the kind of data on which intelligence should focus. Drawing on interview data from an exploratory study on criminal intelligence analysts in Australia, New Zealand, Canada and the United States, we explore participants' perception of datafication, its implications for intelligence practice, and barriers to change. We suggest that datafication has the potential to transform the *epistemic basis* of intelligence practice, but such a transformation is likely to be limited and fraught with challenges. These challenges are primarily *political*, but also have *symbolic* and *material* implications.

The paper is organised as follows. The next section describes the datafication of police intelligence work by drawing on Sheila Jasanoff's (2017) framework on different ideal-type approaches to data representation and their political implications. The section 'Research methods' outlines the methodology used in this research. Section 'The impact of datafication on intelligence practice' describes how research participants perceived the impact of datafication on crime and security information, and the implications for how different intelligence practices are judged. The section 'Barriers to change' discusses the political challenges of changing to a more data-driven approach to intelligence production and the symbolic and material implications of these challenges. The final section summarises the implications of the research findings.

Datafication and intelligence production

Digitisation, datafication and policing

According to Mayer-Schönberger and Cukier (2013: 83), datafication – the transformation of material or information into data that can be recorded, quantified and analysed – should not be conflated with digitisation (which merely converts information into a computer-readable format). Jefferson (2020) does not make this distinction; his research suggests that police (at least in the United States) have started to represent events in the world in the form of data points (for example, in Geographical Information Systems) since the 1960s. Crime occurrence databases have existed even longer.

Empirical research suggests that the adoption of IT has not been a smooth process among police organisations (Manning, 2008). A review of the impact of early 20th century IT on policing concludes that technology has 'fundamentally altered the *field* of policing through the various resources ("capital") it provides and *constraints* ("necessities") it imposes on police work' (Chan, 2003: 664). The implementation and adoption of systems such as computer aided dispatch, records management and geographic information, was described as the 'scientification' of policing aimed to increase officer efficiency,

communication and teamwork (both within and across police services). In general, these technologies have led to both 'changes and continuities in police assumptions about: (1) what police information is for; (2) what is considered relevant information; (3) how information is obtained and used; and (4) how information ought to be obtained and used' (Chan, 2003: 665). Research studies published in the early 2000s found that IT generally did not lead to a more strategic, 'intelligence-driven' style of policing, instead police continue to 'favour case-by-case investigation rather than crime analysis, evidence gathering rather than intelligence analysis, secrecy rather than openness in information sharing' (Chan, 2003: 668). Sanders and Condon's (2017) study, for example, argues that access to analytic platforms and digital information did not alter frontline policing practices, but instead '*reinforce[d]* and *technologically augment[ed]* reactive policing practice' (2017: 13, original emphasis).

Society's demand for risk information (Ericson and Haggerty, 1997), technology's promise of organisational efficiency (Chan, 2003), and the attractions of the rhetoric of 'intelligence-led policing' (Ratcliffe, 2002) have been strong drivers of the *datafication* of information in policing. More recent advances in IT tend towards the exploitation of Big Data, including through artificial intelligence and predictive software. Egbert (2019) argues that the increasing 'platformisation of police work' (i.e. using technological platforms to connect and cross-link diverse data sets) provides more efficient ways for police to retrieve and link previously unconnected data to 'facilitat[e] knowledge creation' and feed into future Big Data projects (2019: 84). Big Data techniques promise opportunities for police services to work more effectively by identifying and predicting crime patterns and offenders in large data sets (Beck and McCue, 2009). Perhaps the most important application of this is 'predictive policing' software that identifies people at risk of offending or being a victim of crime and 'places and times with an increased risk of crime' (Perry et al., 2013: 8–9). Babuta (2017: 19–26) has identified additional uses of Big Data analytics in the United Kingdom for visual surveillance and the analysis of 'open-source data, such as that collected from social media, to gain a richer understanding of specific crime problems'. Some have criticised police's current overreliance on crime analysis for *tactical* work rather than long-term crime reduction (Burcher and Whelan, 2018; Sanders and Chan, 2020). Egbert and Krasmann's (2020: 915) analysis of Germany's PRECOBS software showed how 'current prediction software still strongly echoes the logic of conventional risk technology' that draws on past events to identify high risk areas and employ 'conventional' policing practices.

The central question for this paper is therefore: how has datafication affected which police intelligence practices are valued and what are the barriers to change from one

approach to another? We suggest that changes in intelligence production will require a shift in the epistemic basis of intelligence practice; such a shift would have political, symbolic as well as material implications for police intelligence work. This framework is explained briefly below.

Epistemic basis and the politics of intelligence

To conceptualise the different manifestations of datafication in intelligence production, we borrow from Jasanoff's (2017) analysis of the politics of data representation. Writing in the context of environmental politics, Jasanoff (2017: 2) focuses on the 'legitimacy of the processes of making the invisible visible'. In her analysis of global environmental data, Jasanoff has distinguished three ideal-type 'modes of authorised seeing' or 'regimes of sight' in how information is presented: the *view from nowhere* which claims to be neutral, objective or apolitical; the *view from everywhere* which attempts to be inclusive, rational or representative; and the *view from somewhere* which maintains a subjective, authentic or eyewitness gaze. Each regime carries with it a 'standpoint from which observations are made and explanations provided' (2017: 3), and each involves a specific set of institutional loci, political claims, legitimating discourse and legitimating practices. The 'view from nowhere' is typically associated with science, with its implied objectivity and political neutrality. The 'view from everywhere' is associated with stakeholder advisory bodies, relying on inclusivity and rationality. The 'view from somewhere' is about specific instances of injury or victimisation, the legitimacy of which is based on authenticity. The different regimes of sight are not about automation or reliance on any particular technology but rather about 'what counts as good data within each regime of seeing, counting and accounting for' and depends on 'prior normative choices about such matters as what is worth recording, who is best positioned to collect and report data, and what forms of analysis and representation are taken to be compelling' (Jasanoff, 2017: 3).

Such a framework is applicable to the production of intelligence in policing. It can be argued that the production of intelligence is a process whereby intelligence analysts make certain information visible, meaningful and actionable. Theoretically, datafication can facilitate the move of intelligence production from the 'view from somewhere' to the 'view from nowhere'.¹ The difference between these two regimes of sight can be summarised as follows (see Table 1). The 'view from somewhere' (hereafter VFS), the reactive, personalised, contextualised and case/experience based approach is legitimated by reference to the use of authentic evidence to identify suspects, so justice can be done through arrest and conviction. In contrast, the 'view from nowhere' (VFN), a data-driven,

depersonalised and decontextualised approach to intelligence production is legitimated by reference to the use of 'objective' data (e.g. administrative, social, geographical) and 'scientific' methods to predict threats of crime or disorder. This view sees 'good' data as 'Big Data'. Intelligence work taking this approach claims its validity by purporting to use peer reviewed techniques recognised as scientifically valid, although there may in practice be few independent rigorous evaluations (Bennett Moses and Chan, 2018).

As Jasanoff (2017: 11–12) indicates, each regime of sight is inherently political as each involves *framing* (how questions are formulated), *selection* (where some topics deserve attention while others are overlooked), and *non-knowledge* (relying on what is known while ignoring what is not yet known). This framework suggests that it is important to investigate, for each ideal-type, which forms of knowledge are privileged and the political implications of these choices. For example, it may be argued that VFS is concerned with knowledge specific to an incident; it makes political claims about criminal justice in the sense of holding offenders accountable for causing harm to victims or violating criminal laws, while the validity of the knowledge is either legitimated or contested through peer review (among police and analysts) or, more likely, through the court process. The VFN, on the other hand, is concerned with knowledge that is derived from a larger collection of incidents; it makes claims about political neutrality and objectivity, while the validity of the knowledge claims legitimacy through scientific peer review, evaluation or examination of the underlying assumptions/data. Note, however, that VFS and VFN are ideal-type models that highlight the distinctiveness of each standpoint rather than descriptions of what exists in practice, since both types of knowledge are socially produced and 'situated' (Evans, 2015: 23). The claims that each approach makes to legitimacy do not necessarily apply in practice, so claims relating to objective data or peer review do not mean that the data is in fact objective or that the peer reviewed technique was followed.

We suggest that this VFS/VFN schema is more useful than the well-known distinction between reactive versus proactive policing (Ratcliffe, 2011), tactical versus strategic intelligence (Boba Santos, 2013), and traditional versus evidence-based policing (Cope, 2004). While practical, these distinctions tend to focus on the *styles* and *strategies* of policing rather than epistemic assumptions and political implications. The VFS/VFN schema sharpens analysis by focusing on the limiting cases, that is, what happens if we carry the two regimes to their ultimate extremes? While VFS fits well with 'traditional' policing cultural knowledge (Chan et al., 2003), VFN, which privileges technical capital, potentially changes the *field* of policing and may 'threaten the traditional power structure of an organisation' (Chan, 2003).

Table 1. Applying Jasanoffs (2017) regimes of sight to intelligence production.

Politics stand-point	Claims as to what is worth recording	Claims as to who is best positioned to collect and report data	What forms of analysis and representation are taken to be compelling	Political claim	Legitimising discourse	Quality metrics
View from nowhere	Historical/geographic reports of crime occurrences from police, victims' surveys, academic studies, relevant social data such as hot spot mapping, demographic data from census, social media data.	Science/technology organisations, data scientists, criminal intelligence analysts	Statistical analysis, for example, correlations, predictions, GIS, heat maps, hot-spot analysis, machine learning	Outside politics	Objectivity	Independent, peer review science
View from somewhere	Evidence regarded as sufficient for arrest and charge or admissible in court, for example, eyewitness testimonies, confessions, physical, forensic, expert, or surveillance evidence, social network data	Police, for example, investigators/detectives, field intelligence officers, criminal intelligence analysts	Admissible evidence, for example, photograph, video, sound, document, phone records, witness testimonies, confessions, social network analysis	Criminal justice	Authenticity	Prosecution, conviction

Symbolic capital and material implications of each standpoint

The move from a case-based approach of intelligence production to a more systematic data-driven approach requires more than a change in perspective; the political challenge has implications for police both in terms of symbolic capital and material resources. Chan and Bennett Moses (2019) have synthesised empirical research on policing innovations to highlight the importance of the *organisational*, the *symbolic*, and the *technical* dimensions of technology for understanding the uptake and impact of Big Data approaches. Here, we reconceptualise these factors to two aspects that have implications for implementation and impact: *symbolic capital* and *material resources*.

Symbolic capital refers to the value, legitimacy and prestige placed on different approaches to intelligence production within the police organisation. As Ericson and Shearing (1986: 134) have pointed out, the 'scientification' of policing provides a 'veil of legitimacy over police work'. Similarly, Chan and Bennett Moses (2019: 56) have suggested that '[a]djectives associated with data-driven approaches to decision making (such as "smart" analytics) reflect positively on those who employ them'. A study of the reception of algorithms in policing and criminal courts found that legitimising discourse concerning 'rational' and 'objective' decision making were used to justify their use (Brayne and Christin, 2021). Further, Sandhu and Fussey's (2021) analysis of perceptions of predictive policing technologies found that police leaders and software developers believed that the use of algorithms for assigning patrol officers 'would lessen the exposure of police work to flawed decision making based in human subjectivity and bias...and, therefore uphold objective policing practices' (2021: 73). While predictive analytics have provided symbolic capital to police services, they have also been perceived by police officers as 'deskilling' and 'devaluing' their experiential craft of policing (Brayne, 2017: 14). For example, predictive policing has been found to overlook 'the detailed, contextual, and contingent knowledge that patrolling officers have acquired about their beats' (Ratcliffe et al., 2019: 654). Officers have also expressed concerns that the algorithms would not only replace their discretion and decision-making about patrol (Brayne, 2017; Sandhu and Fussey, 2021), but may also place them 'in direct conflict with deeply felt obligations that were also part of their craft-based knowledge' (Ratcliffe et al., 2019: 654). This line of research draws attention to the technology and craft conflict in predictive policing and how data science practices may threaten the legitimacy of the case-based approach aimed at convictions.

Material resources refer to the availability of financial support, infrastructure and expertise for supporting particular approaches to intelligence production. In adapting intelligence practice to datafication, material support would

include the upgrading of hardware and software and the availability of expertise, training and support in using new techniques and developing new skills. Research available on the material conditions surrounding the production of intelligence has identified significant variation in technological competency and data literacy skills among analysts (Evans and Kebbell, 2012; O'Shea and Nicholls, 2003) and a lack of formal methodological training, core competencies, and accreditation programs (Weston et al., 2019). Further, research on the technological tools adopted for intelligence analysis has identified 'fundamental limitations' to its implementation and effective use. Burcher's (2020) study on the integration and use of social network analysis in policing found that the technological infrastructure of police services posed challenges for producing meaningful analyses and led to the manual manipulation of data which negatively impacted data quality. Babuta (2017) found that fragmented databases and software, along with legal constraints governing data usage and a lack of organisational access to advanced analytic tools, impede the effective use of Big Data analytics (see also Ridgeway, 2017).

In sum, VFN, carried to its logical extreme, means that scientific/technical knowledge and expertise will dominate discourse around intelligence work. Since police organisations typically lack this kind of expertise, they will have to either give up their monopoly over intelligence knowledge or devote resources to buy this kind of expertise and appropriate it for the mission of policing. To maintain the image that police organisations are eager to adopt new technology to improve efficiency and effectiveness, police are likely to invest in technological developments but not VFN in its entirety, hence perpetuating the trend that researchers have found in other studies of policing innovation (Burcher, 2020; Sanders and Condon, 2017), that police will cherry-pick aspects of technology that are symbolically beneficial and financially affordable and employ them to further 'traditional' crime fighting.

Research methods

We base our analysis on data collected for an exploratory international study investigating the work of criminal intelligence analysts in Australia and New Zealand (ANZ), Canada (CAN) and the United States (US). We selected these four countries as they are all members of the 'Five Eyes' intelligence community and have an extensive history of cooperation and information sharing. The study was designed to understand the work of criminal intelligence analysts, their place within law enforcement, the technologies and data sets used, as well as the training, skills and core competencies required of them. In total, we conducted 63 semi-structured, in-depth interviews with analysts, managers of analytical units and field subject-matter experts. Participants included current and past

criminal intelligence analysts working in tactical, strategic and business intelligence capacities, and analysts working in patrol districts and specialty units.

As the first pilot study, ANZ interviews were conducted from August 2016 to December 2016, involving 11 participants from 7 police organisations and 2 experts. In 2017, after receiving additional funding to expand our pilot study, we attended the annual meetings of the International Association of Crime Analysts (IACA) and the Massachusetts Association of Crime Analysts (MACA) where we conducted 15 interviews with US participants representing 15 services (May–July 2017). Canadian interviews were conducted between June 2017 and May 2018, with 37 participants from 8 police services. These samples were not meant to be statistically representative of the population of analysts in the countries mentioned. They nevertheless consist of knowledgeable key informants who were able to comment on current trends in the practice of intelligence production. Our more recent cross-jurisdictional work on police intelligence suggests that the findings presented below are representative of analysts' experiences during this period (Sanders et al., 2020).

Research ethics approval was obtained from both universities, and participants were recruited through: (i) police department participation wherein information about the study was sent to analytic teams with organisational approval to participate; (ii) personal contacts developed at the IACA and MACA annual meetings; and (iii) through key contacts known to the researchers, the snowballing method was employed to reach additional participants with relevant experience. Interview questions explored the background and qualifications of working analysts, training provided, supervision structures, competency evaluation practices, databases accessed, and technological platforms and analytic software used in the production of intelligence. To ensure consistency in data collection practices, the same interview guide was employed (with some role-dependent variation) and an author had meetings with the research assistants during the data collection phase to share analytical insights.

Interviews were digitally recorded and transcribed verbatim. The Canadian research assistant coded and analysed all data using a reconstructed grounded theory approach (Charmaz, 2006) that involved an iterative and constant comparative method, which was grounded in the data but also attentive to existing theoretical insights from the literatures on police intelligence analysis (e.g. police cultures) and science technology studies (e.g. regimes of sight, symbolic capital). Using NVivo11, a qualitative data analysis software, the data were initially coded categorically – some categories followed specific areas of interest in the interview guide (such as technological platforms) and some emerged through participants' experiences (such as sensemaking). To move our coding to a deeper level analysis, the lead author drafted analytic memos to compare

data, contexts and categories in order to see if and where variations existed, and to identify thematically and analytically coherent interpretations of the practice of intelligence analysis (Charmaz, 2006).

While the organisation of police services varies substantially among the countries we studied, the work experiences and challenges encountered by analysts were similar. Both the US and Canada, for example, have services that are much more localised than those in Australia, whereas New Zealand has only one police service. At the time of data collection, all four countries were working to professionalise intelligence roles and seeking to standardise practitioner qualifications – with most looking to the IACA for training and professionalisation. As such, the professional state of criminal intelligence analysis was similar across the four countries. To demonstrate this similarity in our findings, we have purposefully included data from each jurisdiction. Through analytic memos, we were also able to identify where variation does exist. Although there were differences caused by differing governance structures and privacy legislation, the variation was not so much by jurisdiction as connected to participants' role and position within the organisation. For example, intelligence analysts holding management roles or working in strategic intelligence units had a slightly different mode of seeing as compared to district level crime analysts and those working in tactical units. However, considering the sample sizes relative to the numbers and sizes of police organisations in the four countries, we are unable to make observations regarding variations *between* organisations and countries. Instead we encourage other researchers to draw upon our findings to conduct a broader cross-jurisdictional comparative analysis.

The impact of datafication on intelligence practice

In this section, we draw on empirical data to investigate how datafication has affected intelligence practice in the countries included in our research. We report on participants' perceptions of datafication and its impact on the perceived value of different approaches to intelligence.

Perception of datafication

Participants saw technological change as both a cause and a cure of the proliferation of the volume of information. For example, agencies used to work with paper-based records ('index cards, paper files, paper maps' [ANZ]). With the introduction of digital computers, the initial change was no more than digitising a paper process; datafication came much later:

So I think initially there's that we need to make the records electronic and so there's just this digitization of what

essentially is a paper process. Then there's moving to the data paradigm where you're actually treating the information coming in much more as data ... bits of information that you can manipulate in many different ways. (ANZ)

Participants saw technological change in terms of the *volume of data* they need to manage and analyse. One participant recounted the scale of change in their organisation:

10 years ago we were dealing with things that could fit on a flash drive ... Where[as] now it's filling up server farms of data... (CAN)

With the increasing volume of data, analysts also noticed a change in technological platforms that would allow them to search, query and analyse across platforms. ArcGIS, i2, Access, Excel and Palantir were the most commonly referenced and used platforms by analysts. As one Canadian analyst explained,

I use i2 and Palantir, more or less every day. [Palantir] is an intelligence tool that can access different databases. And it brings it all together. So, it works with our records management system, to pull together different bits of information on persons. So being in the intelligence unit, we deal with organized crime, terrorist networks ... so it is a very useful tool for us, in that we can pull in all of our subjects of interest, and do criminal associates searches. So, we can get the network. Then we can take that information, plug it into i2, do social network analysis, and provide central actors. (CAN)

This suggests that the interoperability of databases was perceived to enhance intelligence work by providing access to larger data sets from disparate systems that would enable analysts to do advanced searches as well as analysis.

With increased access to data and technological platforms, analysts discussed how skill sets varied between *types* of analyst positions. For example, a strategic analytic supervisor describes how the skills required for a strategic unit differ from those in tactical positions:

The skills that I'm really looking for in a prospective [strategic] analyst is data expertise.... The more research type of stuff. Whereas the tactical is gonna understand more things like threat assessment and more operational applicable stuff. (CAN)

Hence, different analytic positions require different data literacy skills, which in turn has created significant *variance* in analyst skill sets in practice. As a Canadian business strategist for analytics explained:

Our initial thought of implementing the business intelligence tool is that it would be ... a one stop shop, and any [analyst] could have the privileges to go in and build the reports ... what it has become is that we have a group of about 8 people that we trust with data skills who can build reports for the other 80 people to use ... but they cannot build a report because if they build the report then the likelihood of them getting a wrong answer is high ... they need to understand data models. (CAN)

Analysts often discussed how they spend most of their time creating 'daily reports, briefings, subject profiles, information about particular people or groups, [and] problem profiles' (ANZ), as well as 'heat lists' (US) and 'hot spot maps' (CAN). Further, they explained how less time is spent conducting social network analyses or other structured analytic techniques, such as visualisation, challenging assumptions and group processes that assist analysts in overcoming cognitive pitfalls (Pherson and Heuer, 2020). As the following analyst complained,

SNA is the only structured analytic technique that should be used in looking at organized crime. But, we don't do that. All we do is draft up chronologies, and timelines and, 'look at this fancy chart where I have all the guys' pictures on it'. That is analyst's work. (CAN)

The smaller number of analysts who did speak about using advanced data science practices were those working as intelligence managers or strategic intelligence analysts.

Although user capability varied significantly among analysts regardless of country, datafication (together with related technological advances) was perceived to have improved police intelligence work by enhancing analysts' abilities to search, store, query and analyse across multiple data bases simultaneously.

Perceived value of different approaches to intelligence

As information is increasingly datafied, contextualised reports can be disaggregated and treated as raw data for future analysis, so that the distinction between information and data has disappeared, according to most of the research participants. In contrast, participants saw 'intelligence' as qualitatively different from information or data. As one analyst explained, information provides the little 'i' of intelligence, while the ability to pull disparate pieces of information together and analyse it provides the big 'I' of intelligence:

the value comes when you've got that intelligence product which pulls together multiple intelligence submissions alongside the criminal code information, alongside ... record source information, that generates inferences,

recommendations... and to me this is the "big I" intelligence. And I think historically when we talked about intelligence ... we spoke about little 'i' intelligence. And having the [analytic software] come in has allowed us to... start delivering big I Intelligence. (CAN)

Many analysts described intelligence as something that has value added:

Intelligence is really about adding value to that information, or data. Intelligence is about ... providing insight during times of uncertainty. So it's stepping a long way beyond the data and the information we have. (ANZ)

In this way, the analysts use their knowledge, judgement and experience to make sense of the data and information they work with. The practice of intelligence production can be framed in terms of *both* individual cases *and* patterns of offending:

So normally [analysts] get a task They'll go about trying to collect the data ... They then go about trying to answer normally very specific questions of who's this guy in contact with on the phone or email or communications, who else might he be associated with, looking for patterns or lack of patterns or absences. (ANZ)

This suggests that the analyst collects and analyses data to answer questions about *a specific individual and their associates*, presumably for the purpose of identifying patterns and roles played by individuals. Nevertheless, the analyst is also 'looking for patterns' of offending or association between offenders. The following participant demonstrates how analysts 'add value' through the analysis of years of data to look for trends that can assist with identifying suspects:

One of my analysts has done an amazing job at creating a matrix where she has looked at 14 homicides, as well as a whole host of shootings, stabbings, home invasions, extortions and kidnappings. ... So now ... we can do frequency distributions on how many of those offenders are coming up the most put together some key sort of people that we can say, these guys right here, based on a social network analysis, seem to be your key guys. (CAN)

Note, however, that while this analysis of aggregated data is facilitated by datafication, especially the integration of data sources, it is a less ambitious or sophisticated form of prediction compared with some of the promises of machine learning techniques (cf. Jefferson's (2020) history of police use of GIS).

The push towards datafication and the integration of technological platforms and analytic methods provides police services with an opportunity to move away from

VFS that is primarily focused on a particular crime or suspect and motivated by the needs to collect evidence and secure a conviction, towards VFN that purports to use data science to ‘objectively’ analyse trends to predict and disrupt crime.

... The height of intelligence is predictive, so we’re trying to predict the future or provide information in a way that people can operationalise it and affect the future ... whether it’s a national opportunity that we may be able to exploit for national benefit, or to prevent a threat... (ANZ)

As one Canadian intelligence manager explained,

We’re also doing predictive policing ... So, we do crime forecasting on property crime... we have dedicated teams that are deployed out every morning from 8 in the morning till 4 in the afternoon to forecasted locations and based on that we’ve had significant reductions in property crime.... we’re bringing in everything from weather data to ...corrections, we have that MO typology for sex crimes, robbery assault and property crime ... we bring in social media into that ...we use an IBM product which does unstructured data ingestion. (CAN)

IT and data analysis were perceived as being valuable for predicting where crime was going to happen or who was engaging in serial offences. The following quote further illustrates this shift from ‘good intelligence’ for assisting with convictions and arrests towards ‘good intelligence’ for predicting where and when crime will occur, or where a possible suspect may reside:

At the heart of geographic profiling ... it’s taking sort of a set of linked offences to try and figure out an anchor point ... So we take offenses like that and then overlay some fancy algorithms and use a geographic profiling software to identify where he might live or work or hangout. (CAN)

A team-based approach to intelligence production, where people from different units with different types of information worked together to make sense of the problem, was seen as effective for providing a more holistic picture:

So we have our drug analyst who has been more on the tactical side, pulling together what she sees as trends, and giving descriptions of what types of drugs are out there. We have other analysts looking at what are the correlations between ... drug offences and overdoses and other criminal activity. We have another one looking at what impact this has had for our calls for service and then looking at costing. We have had other [analysts] do maps ... [on] spatial analysis component ... so I think the future of our reports ... is that it is a compilation, it is looking at it from different lenses. ... and then pulling all those pieces

together creates the bigger picture ... of what are our drug issues. (CAN)

This approach has the potential to bring together VFN and VFS. While all participants could see the potential for police intelligence practices to move toward VFN, a smaller number of analysts actually perceived this change to be occurring in practice: these were largely intelligence managers.

Competing regimes of sight?

The above analysis suggests that datafication does not by itself lead to the privileging of the VFN model of police intelligence practice. A complete shift from traditional policing (VFS) to VFN is patently not happening. Perhaps pragmatically, the two regimes of sight may *co-exist* in policing intelligence practices, but the latter is almost always at the service of the former. For instance, when asked for an example of a good intelligence product, many analysts would describe using advanced analytical practices for the purposes of collecting evidence for making arrests and convictions.

I’m the SNA guy, so I was given the list of targets. I plugged them into Palantir, and looked at all the criminal associations. And then, I took that and put it into i2 and found out who the central actors were. Then, I gave them ... a vector closeness degree score and ranked them, and said ‘these are persons that should be targeted for intelligence, because they are well suited within the criminal network’. (CAN)

While datafication has proceeded rapidly, as illustrated above, a focus on individuals continues to play an important role and data science techniques continue to be seen as useful only for identification of suspects. As one analyst lamented,

what we really need to do is not be focusing on one guy, but to be able to ask meta questions. Like, find the guy, within these datasets. If you didn’t know his name already, who would be the number one person we gotta focus on as likely being involved in some sort of terrorist activity, given these millions of people we have in all these different databases? That’s where the rubber meets the road, when it comes to your ability to synthesize and link to all the different databases that you need. And I just don’t see anybody doing that. (US)

Barriers to change

To understand why the shift towards VFN is fraught with challenges for crime intelligence, we explore interviews with participants that identify substantive barriers to this

kind of change. These intertwined barriers, in keeping with Jasanoff's framework, are primarily political, but have symbolic and material implications (Chan and Bennett Moses, 2019).

Political barriers

The politics of data refers to the battle that occurs between the institution of policing and its 'experiential knowledge' of crime, and the insertion of technology companies that operate on their own epistemic space. The following quote by a crime analyst speaks to this 'politics of data' wherein we see a contention between police and tech companies regarding who should legitimately produce intelligence:

... Based on what my findings were, we didn't renew our contract [with the tech company]. ... it didn't tell us anything that we didn't already know. ... They produce a map every day... So that map, and the boxes on that map, and the addresses, were always the same boxes that we already knew about. Every now and then we'd have a weird address on there, ... And we wouldn't have a call there, in 5 years. So I would question them saying – why is this even on here? ... How do you justify pulling people out of areas that you know are hot and busy that you're going to have a crime in, to go sit ... in an area that's never had a crime? (US)

This type of conflict between technology and the experiential craft of patrol policing is consistent with research on patrol officers' perceptions of predictive policing (Brayne, 2017; Krasmann, 2020; Ratcliffe et al., 2019; Sandhu and Fussey, 2021). The quote above also highlights the importance of the 'involvement of human decision making and assessment' for the effective use of predictive analytics (Egbert and Krasmann, 2020: 910). As illustrated above, when police were unsure about how accurate and effective the predictions were, they no longer supported the use of the software.

Just as there was a politics of data around the experiential knowledge of crime and tech companies, many analysts noted a similar conflict between analysts and police managers.

[Police organizations] are very much hierarchical with command structure and analysts are a tack-on, add-on kind of adjunct to that mechanism and not known to be front and centre driving any processes and technology aside, that's the bigger challenge in law enforcement in my view. (CAN)

... Intelligence and policy are basically separate processes ... in certain policing agencies, they want the analysts to go further, to make implications and recommendations,

but in other agencies they don't, because the senior command don't want to be told by analysts what to do. It's a cultural thing. (ANZ)

As the ANZ analyst explains, a political tension exists between analysts, who are tasked with constructing intelligence products, and managers who want to control what recommendations arise from the intelligence product.

Further, when we asked analysts about the use of analytics for strategic intelligence purposes, many noted that their service did not invest fully in such practices because of the case-based targeted approach and the political nature of policing. Specifically, analysts discussed how the pressure for police services to demonstrate 'wins' through big arrests and seizures often forced analysts to operate within a case-based approach.

Even [in] our bigger investigations there is less of an appetite [for strategic analysis] because of the resources that are involved. So, as an analyst, we could pool all of that information and start seeing the connections and identifying what works – pull financial of these individuals and see where the money is coming and going ... We don't have the resources because we don't have forensic accountants that are capable. ... so there is no appetite for that ... (CAN)

Symbolic barriers

Appreciating the value of data. According to one of the experts we interviewed, law enforcement agencies are only now beginning to see the value of data for prediction and trend analysis, lagging behind national security agencies:

There's a lot more data being used by law enforcement agencies than some of the national security agencies, but I suspect [it] isn't being used very well, and so there's probably a lot more data that's held by the law enforcement agencies around the country, particularly high-volume crime areas and stuff, but it's probably residing in information silos still ... But the law enforcement agencies are catching up ... (ANZ)

Trust in civilian staff. Another barrier to change was the relationship of trust. Consistent with existing research on the work of intelligence analysts (Cope, 2004; Sanders and Condon, 2017), our participants discussed how civilian analysts did not always have access to information because they were not trusted by sworn staff. Even though new technological platforms are being implemented to facilitate information sharing, our findings identify the important role 'trust' and organisational 'symbolic capital' play on the integration of analytics. The lack of symbolic capital afforded to civilian analysts has led their work to be

undermined and underutilised (see also Fraser and Atkinson, 2014; Innes et al., 2005). Of particular interest in our findings is the differential access of symbolic capital afforded analytic technologies (i.e. smart tools) as compared to intelligence analysts who often represent the antithesis of operational police culture (Atkinson, 2017).

Material barriers

Access to data and resources. While participants referred to changes to intelligence work as a result of advancement in technology and access to increased volumes of data, our data shows how these changes varied by organisations and jurisdictions. At a time of technological change, differential access to data and resources means that the distribution of technological capital (expertise and tools) would be uneven, with some agencies well ahead of the game and others left behind. This unevenness in distribution across agencies has implications for the extent to which the game of intelligence production can be played in the same way.

For example, in police departments without access to integrated information systems, intelligence work can be frustrating:

So one of my biggest frustrations is I can have like seven different law enforcement databases open, and for security reasons, they're all different passwords. (US)

The need for better system integration and data quality was echoed by participants in other jurisdictions:

I think our technical support needs to improve across the board. I think I made reference to the 15 to 20 databases that we have ... Well, we also have disparate computer systems that don't all speak to each other ... (ANZ)

In contrast, a participant from a jurisdiction which was far advanced in terms of technological development, had access to infrastructure and a skill set of analysts that he described as 'mind boggling':

Yeah, just [the] skill set that's coming in the door now ... It's interesting. My most recent hiring on a GIS specialist ... I've got a cadre of mathematicians that work in the strategic analysis ... These guys are writing algorithms in our code that can deconstruct data and find patterns in it, and they'll write this in a weekend. ... It's scary. (CAN)

Our data demonstrates variations in the level of technical interoperability, sophistication and data literacy skills amongst police services that, in turn, shapes the ability of each service to effectively integrate and use analytic practices.

Technical expertise. Our interviews also suggest that money was often not spent wisely on technology because of police management's lack of understanding of the role and needs of intelligence analysts:

Often what happens, though, is that these things are bought by management that's not necessarily understanding intelligence, what an intelligence analyst needs, and you get this sort of thing that's just plonked on someone's desk and say well, that's what we've bought. (ANZ)

As another participant pointed out, there were managers who knew the intelligence 'business' well but lacked a good understanding of technology:

... you've got managers who are very good at the business... technology's always just been there to support them. They're the guys now controlling multimillion dollar budgets about making huge strategic decisions on which technology path to go down. That's really hard. (ANZ)

The quotes above draw attention to the uneven distribution of technological capital within the field of policing, as well as the changing skill sets required for new data-driven tools to be effectively integrated and used within law enforcement. One of the reasons for the inadequate supply of technical expertise relates to training. Several participants across all countries described an *ad hoc* approach to training:

... This latest round of training from the Bureau of Justice Assistance here in the US has been the only sustained effort that I know of to teach police executives and administrators about crime analysis and what they should be expecting from it ... the FBI National Academy ... and various leadership institutes have occasionally had a class or two in crime analysis. But again, in no standardized way. (US)

Lack of analytical and technological training renders many services unable to utilise their analytic capabilities effectively.

Such experiences demonstrate how data analysis was not adequately 'embedded' (ANZ) within the organisation, which reduced the impact of the work:

... Some of the Sergeants don't even look at the bulletin. ... they're literally looking through the dispatch log and looking into every report. And I'm like – I've already done that for you. And I added pretty pictures [laughs]! So there's just zero communication and there's ... no directive. (US)

The material barriers, such as poor technological interoperability, technological expertise and data literacy skills, are consistent with the broader literature on intelligence analysis (Belur and Johnson, 2016; Burcher and Whelan, 2018; Innes et al., 2005). Our findings further support criticisms regarding the lack of a strategic and standardised approach to analytical training (Walsh, 2011) that have created impediments to the uptake and use of analytic practices in policing.

In summary, our analysis suggests that the barriers to change perceived by participants are predominantly political, involving a contest of expertise and resourcing between the craft of policing and the science of data analytics. Part of this contest is played out symbolically within police organisations reflecting differences in approaches (strategic vs tactical), values and trust between sworn police officers and civilian crime and intelligence analysts. The contest is manifested in competition for data and technical resources, constituting material barriers that impede the adoption of a more 'scientific' approach to intelligence production. These barriers explain the formidable challenges in any substantive change from current practice to an ideal VFN approach. Our preliminary exploration provides evidence that, similar to the way police organisations take up other technological innovations, the VFN, if it is adopted at all, is likely to be used as a tool to serve the needs of case-based intelligence practice, the VFS.

Conclusion and implications: the politics of intelligence practice

This paper has used empirical data on criminal intelligence analysts in four countries to identify how datafication has affected the practice of intelligence production. We have argued that advancement of data science in recent years has given rise to two competing 'regimes of sight' (Jasanoff, 2017) in intelligence production: the case-focused VFS and the data-driven VFN. Each regime of sight is aligned with a particular form and site of power. Case-based intelligence practice (VFS) privileges the expertise of police intelligence personnel, and the power of the criminal justice system to effect justice at the individual level. Data-driven intelligence practice (VFN) privileges ideas associated with data science and the power of technology and use of smart tools to produce predictions at a geographical or temporal level. Embedded in both regimes of sight are the political mechanisms of framing (e.g. what questions are asked), selection (e.g. what models or theories are used) and non-knowledge (e.g. the unknown unknowns) (Jasanoff, 2017: 11–12). Criminal intelligence is a form of knowledge about crime; this knowledge is shaped by these processes of framing, selection and non-knowledge in both regimes of sight:

The view-from-nowhere approach tends to obscure the fact that such influences are at work behind allegedly neutral protocols for generating policy-relevant knowledge. By denying the influence of values and judgment, this approach leaves itself open to charges of corruption whenever the stage curtain of science slips and the values behind are unexpectedly revealed. The view from somewhere insists on making the politics of knowledge-making visible, but potentially at the expense of rigor and sustained intellectual self-critique. (Jasanoff, 2017: 12)

During a time of considerable public debate about both the role of police and the fairness and efficacy of police practices, empirical research into the production of police intelligence is crucial to ensure there is not technological overreach (McGuire, 2020). It is clear that each regime of sight has its own blind spots; it is important to be aware of these weaknesses. To ensure truly 'smart' intelligence in an age of datafication, criminal intelligence knowledge must be subject to contestation, not only through rigorous peer review/rival hypothesis testing in intelligence process or the testing of evidence in court (as with VFS), but also the questioning of assumptions and data underlying algorithms (as with VFN). There is by now a critical literature that questions the validity and fairness of some Big Data prediction techniques and smart tools (Bennett Moses and Chan, 2018; Browning and Arrigo, 2021; Ferguson, 2017). The veil of neutrality has been lifted to expose some of the inappropriate assumptions and underlying bias of prediction techniques. As a source of knowledge about crime, its objectivity and neutrality has been challenged. This is not to imply that VFS is in any way a satisfactory source of knowledge about crime. It is subject to many processes of framing (e.g. law and order politics), selection (e.g. non-enforcement of certain offences at certain times, resource constraints) and non-knowledge (e.g. the neglect of family violence and corporate crime). Apart from testing evidence in court, there are well-established 'best practices' in intelligence analysis either through peer review or the testing of rival theories ('red teams', see Quarmby and Young, 2010: 135; Walsh, 2011: 238) that can challenge the validity of case-based intelligence. While contestation is necessary, it is not sufficient (see, e.g. Van Brakel, 2020), given the political nature of intelligence production.

By employing Jasanoff's schema to conceptualise and make sense of the effect datafication has had on policing, we have exposed the political nature of intelligence production by identifying the intertwined barriers to change. Specifically, we have identified challenges associated with the political nature of data practice, which is partly manifested in the symbolic capital accorded experiential knowledge over data-driven intelligence production and partly responsible for deficits in material conditions such as technological knowledge and skill, poor technological

integration and interoperability. Each of these challenges raise ethical concerns regarding transparency and accountability of police decision-making and operations (Egbert and Krasmann, 2020). Indeed, the constructed nature of police intelligence becomes sanitised and the ‘observational standpoints and associated political choices that accompany any compilation of authoritative information’ become black-boxed and rendered invisible (Jasanoff, 2017: 12).

Previous studies (Chan, 2003; Sheptycki, 2004) have suggested that the introduction of police intelligence has always been fraught with tension between the imperative to arrest/convict a culprit (VFS) and the ideal of intelligence to take a broader view (not necessarily VFN, but something more in line with problem-solving policing, taking into account social, demographic, environmental factors in identifying risks). VFN is not a recent development, early manifestations can be found in the use of crime mapping, intelligence-led policing, or evidence-based policing. The most recent and most extreme manifestation of VFN would be examples such as predictive policing where policing strategies are *determined* by data-driven algorithms. As long as science/technology is an ally of policing, it is subordinate to policing imperatives, so that VFN needs to serve the imperatives of VFS. The danger with the most extreme form of VFN from the perspective of police is the need to give up the monopoly of legitimacy/symbolic capital that once was theirs and subordinate it to or share it with for profit technology companies. Police organisations that are too dependent on technology will then need to sacrifice material resources such as police personnel and traditional policing equipment to acquire technological expertise and infrastructure. So, there is a trade-off. Our exploratory study suggests that a complete shift from VFS to VFN is not likely to happen but that the two models might co-exist within police services. In this scenario, VFN serves VFS, resulting in further tension between sworn officers and civilians, organisational inertia or technologies that are under-utilised or abandoned.

Acknowledgements

We wish to thank all the experts and analysts who took time out of their busy schedules to participate in this research. We are also thankful for the research assistance provided by Andrea Corradi, Crystal Weston and the Centre for Research on Security Practices (CRSP).

Declaration of conflicting interests


The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.


Funding


The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by a University of New South Wales Law

Faculty Research Grant (2016) and a Social Sciences and Humanities Research Councils of Canada Insight Grant.

ORCID iDs

Carrie Sanders  <https://orcid.org/0000-0001-8533-0129>

Lyria Bennett Moses  <https://orcid.org/0000-0003-2571-1469>

Holly Blackmore  <https://orcid.org/0000-0003-0337-8896>

Note

1. The ‘view from everywhere’ is currently absent in debates about data for police intelligence.

References

- Atkinson C (2017) Patriarchy, gender, infantilisation: a cultural account of police intelligence work in Scotland. *Australian & New Zealand Journal of Criminology* 50(2): 234–251.
- Babuta A (2017) Big data and policing: an assessment of law enforcement requirements, expectations and priorities. RUSI Occasional Paper. Available at: <https://rusi.org/publication/occasional-papers/big-data-and-policing-assessment-law-enforcement-requirements> (accessed 15 March 2021).
- Beck C and McCue C (2009) Predictive policing: what can we learn from Wal-Mart and Amazon about fighting crime in a recession? *The Police Chief* 2009: 18–24.
- Belur J and Johnson S (2016) Is crime analysis at the heart of policing? A case study. *Policing & Society* 28(7): 768–786.
- Bennett Moses L and Chan J (2018) Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing & Society* 28(7): 806–822.
- Boba Santos R (2013) *Crime Analysis with Crime Mapping*. 3rd ed. Los Angeles: Sage Publications.
- Brayne S (2017) Big data surveillance: the case of policing. *American Sociological Review* 82(5): 977–1008.
- Brayne S and Christin A (2021) Technologies of crime prediction: the reception of algorithms in policing and criminal courts. *Social Problems* 68(3): 608–624.
- Bright D and Whelan C (2020) *Organised Crime and Law Enforcement: A Network Perspective*. London: Routledge.
- Browning M and Arrigo BA (2021) Stop and risk: policing, data, and the digital age of discrimination. *American Journal of Criminal Justice* 46(1): 298–316.
- Burcher M (2020) *Social Network Analysis and Law Enforcement: Applications for Intelligence Analysis*. Cham, Switzerland: Springer.
- Burcher M and Whelan C (2018) Intelligence-led policing in practice: reflections from intelligence analysts. *Police Quarterly* 22(2): 139–160.
- Chainey S, Tompson L and Uhlig S (2008) The utility of hotspot mapping for predicting spatial patterns of crime. *Security Journal* 21: 4–28.
- Chan J (2003) Police and new technologies. In: Newburn T (ed) *Handbook of Policing*. Cullompton: Willan, 655–679.
- Chan J, Bennett Moses L (2019) Can ‘big data’ analytics predict policing practice? In: Hannem S, Sanders C, Schneider C, et al. (eds) *Security and Risk Technologies in Criminal Justice: Critical Perspectives*. Toronto: Canadian Scholars Press, 41–86.
- Chan J, Devery C and Doran S (2003) *Fair Cop: Learning the Art of Policing*. Toronto: University of Toronto Press.

- Charmaz K (2006) *Constructing Grounded Theory*. London: Sage.
- Cope N (2004) Intelligence led policing or policing led intelligence? Integrating volume crime analysis into policing. *British Journal of Criminology* 44: 188–203.
- Dencik L (2019) Situating practices in datafication – from above and below. In: Stephansens HC and Treré E (eds) *Citizen Media and Practice*. London: Routledge, 243–255.
- Egbert S (2019) Predictive policing and the platformization of police work. *Surveillance & Society* 17(1/2): 83–88.
- Egbert S and Krasmann S (2020) Predictive policing: not yet, but soon preemptive? *Policing & Society* 30(8): 905–919.
- Ericson R and Haggerty K (1997) *Policing the Risk Society*. Toronto: University of Toronto Press.
- Ericson R and Shearing C (1986) The scientification of police work. In: Bohme G and Stehr N (eds) *The Knowledge Society. Sociology of Science Yearbook, Volume 10*. Dordrecht: Reidel, 129–159.
- Evans R (2015) What is expertise? Technical knowledge and political judgement. In: Berling TV and Bueger C (eds) *Security Expertise: Practices, Power, Responsibility*. Abingdon and New York: Routledge, 19–36.
- Evans J and Kebell M (2012) The effective analyst: a study of what makes an effective crime and intelligence analyst *Policing & Society* 22(2): 204–219.
- Ferguson A (2017) *The Rise of big Data Policing: Surveillance, Race, and the Future of law Enforcement*. New York: New York University Press.
- Fraser A and Atkinson C (2014) Making up gangs: looping, labeling, and the new politics of intelligence-led policing. *Youth Justice* 14(2): 154–170.
- Innes M, Fielding N and Cope N (2005) The appliance of science? The theory and practice of crime intelligence analysis. *British Journal of Criminology* 45: 39–57.
- Jasanoff S (2017) Virtual, visible, and actionable: data assemblages and the sightline of justice. *Big Data & Society* 2017: 1–15.
- Jefferson B (2020) *Digitize and Punish: Racial Criminalization in the Digital Age*. Minneapolis: University of Minnesota Press.
- Krasmann S (2020) The logic of the surface: on the epistemology of algorithms in times of big data. *Information, Communication & Society* 23(14): 2096–2109.
- Manning P (2008) *The Technology of Policing: Crime Mapping, Information Technology, and the Rationality of Crime Control*. New York: New York University Press.
- Mayer-Schönberger V and Cukier K (2013) *Big Data*. London: John Murray.
- McGuire M (2020) The laughing policebot: automation and the end of policing. *Policing and Society* 31(1): 20–36.
- NASEM (National Academies of Sciences, Engineering, and Medicine) (2019) *A Decadal Survey of the Social and Behavioural Sciences: A Research Agenda for Advancing Intelligence Analysis. Consensus Study Report*. Washington DC: The National Academies Press. Available at: <https://doi.org/10.17226/25335>.
- O’Shea TC and Nicholls K (2003) Police crime analysis: a survey of US police departments with 100 or more sworn personnel. *Police Practice and Research* 4(3): 233–250.
- Perry WL, McInnis B, Price CC, et al. (2013) *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Washington, DC: RAND Corporation.
- Pherson RH and Heuer RJ Jr (2020) *Structured Analytic Techniques for Intelligence Analysis*. Los Angeles: CQ Press.
- Quarmby N and Young LJ (2010) *Managing Intelligence: The Art of Influence*. Sydney: Federation Press.
- Ratcliffe J (2002) Intelligence-led policing and the problems of turning rhetoric into practice. *Policing & Society* 12(1): 53–66.
- Ratcliffe J (2010) Crime mapping: spatial and temporal challenges. In: Piquero AR and Weisburd D (eds) *Handbook of Quantitative Criminology*. New York: Springer, 5–24.
- Ratcliffe J (2011) *Intelligence-Led Policing*. New York: Routledge.
- Ratcliffe J, Taylor R and Fisher R (2019) Conflicts and congruencies between predictive policing and the patrol officer’s craft. *Policing and Society* 30(6): 639–655.
- Ridgeway G (2017) Policing in the era of big data. *Annual Review of Criminology* 1: 401–419.
- Sanders C and Chan J (2020) Challenging the effective integration and use of big data analytics in Canadian police. In: Lyon D (ed) *Security in the Era of Big Data*. Vancouver: University of British Columbia Press, 180–194.
- Sanders C and Condon C (2017) Crime analysis and cognitive effects: the practice of policing through flows of data. *Global Crime* 18(3): 237–255.
- Sanders C, Weston C, Bennet Moses L, et al. (2020) Conceptions of intelligence: studying police intelligence practices and frameworks in Australia, Canada, and New Zealand. Project Report (34 pages).
- Sandhu A and Fussey P (2021) The ‘uberization of policing’? How police negotiate and operationalise predictive policing technology. *Policing & Society* 31(1): 66–81.
- Sheptycki J (2004) Organizational pathologies in police intelligence systems. *European Journal of Criminology* 1(3): 307–332.
- Smith G, Bennett Moses L and Chan J (2017) The challenges of doing criminology in the big data era: towards a digital and data-driven approach. *British Journal of Criminology* 57(2): 259–274.
- Van Brakel RE (2020) Een reflectie over het huidige toezicht van het gebruik van surveilancetechnologie door de lokale politie in België. *Cahiers Politiestudies* 55: 139–160.
- Walsh PF (2011) *Intelligence and Intelligence Analysis*. London and New York: Routledge.
- Weston C, Bennett Moses L and Sanders C (2019) The changing role of the law enforcement analyst: clarifying core competencies for analysts and supervisors through empirical research. *Policing & Society* 30(5): 532–547.