Helene Oppen Ingebrigtsen Gundhus and Jenny Maria Lundgaard

33 Intelligence

Abstract: Intelligence can be understood as an organizational activity and a power process, where security and powers are enhanced by identifying what is believed to happen in the future, in the absence of countermeasures. This chapter looks at the origins and meaning of the term and shows how intelligence can be framed both as a process, as a product, a managerial effort, and as practice. As intelligence depends on information gathering and is heavily influenced by the information technologies used, new forms of digitalization make intelligence an intriguing field for criminologists interested in the production and use of knowledge by states, in law enforcement, or elsewhere.

Keywords: datafication, intelligence, policing, security, surveillance

The term 'intelligence' is often associated with secret agents fighting enemies on behalf of a state. Whilst realities are seldom as exciting as fiction, the secretive and intrusive nature of intelligence, where information is gathered to map, reveal, predict, and prevent something unwanted, is full of important topics for criminologists to explore, especially as more of these practices are closely linked to the use and development of technological and digital platforms and systems.

Information gathering used by and against states is nothing new. With references to the Bible, ancient China, and the reign of Queen Elizabeth I, Buckley (2013) shows the constancy of such activities, as well as showcasing the problematics embedded in them, as intelligence practices can deprive citizens of their rights, instead of protecting these rights. The history and development of intelligence and intelligence agencies have been linked to the large wars of the last century (Buckley, 2013). However, current intelligence is not only a military affair. The collection of information for intelligence purposes is embedded in the activities of state departments and agencies, corporate profitmaking corporations, and non-governmental organizations (Gill and Phythian, 2018). As we will show later, intelligence practices and methods are influenced by technological advances that present us with new challenges (Clemente, 2014). As intelligence is carried out within multiple state agencies it is also directed against various phenomena, from matters of war to national security, and in the policing of various forms of crime, which is this contribution's main focus. From the early 2000s, intelligence-led policing has been implemented as a strategy in several police forces (Fyfe et al., 2018; Gundhus et al., 2022; Ratcliffe, 2016). Ratcliffe (2016) argues that this was a result of a strive towards efficiency and professionalization of policing, but geopolitical

Project funding: This research is partially funded by the Research Council of Norway, grant: 301762 and grant: 313626

Open Access. © 2025 the author(s), published by De Gruyter. BY-NC-ND This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. https://doi.org/10.1515/9783111062037-034

factors, such as the aftermaths of the Cold War and the terrorist attacks of 9/11, have also fueled this shift, as have technological developments (Sheptycki, 2004).

Research on intelligence has been extensive within the school of international relations and defense studies, and so have historical accounts provided by former intelligence officers (Gill and Phythian, 2018). However, we find fewer historical analyses of intelligence within the field of policing (Ellefsen and Lomell, 2024). James (2013: 5) shows that intelligence activities within specialized police units in the UK date back to the 1880s. Ellefsen and Lomell (2024) use a broader concept, illustrating that intelligence practices are not only a modern concept, because systematic information gathering and reporting activities have been a police task since the first police offices were established at the end of the 17th century, showcasing how the term intelligence is rather abstract and shaped by historical connotations and origins. However, information gathering has historically often been dependent on technology. Therefore, as practices become increasingly digitalized, there is a continuum of intelligence practices and technologies, even if the digital component is new.

The elusive term 'intelligence'

In 1949 the founder of modern intelligence studies, Sherman Kent, defined intelligence as consisting of three overarching elements: intelligence is *knowledge*, produced in a *particular kind of organization or enterprise* that *performs particular intelligence activities* (Kent, 1966). We here include a fourth and often underlined element, namely that *the activities have a particular purpose or function* in mind. In the thirty definitions of intelligence found by Rønn (2016), these elements were present, but the definitions also aimed to include new perspectives. Following the traces of the concept intelligence, it stands out as dynamic, elusive, and easily adapted to various environments. There is no agreement on how to define intelligence across different contexts, but common through history seems to be "know your enemy," and something that is "a means to an end" (Gill and Phythian, 2018: 1). The most comprehensive definition and perhaps the most cited, Gill and Phythian's, is of particular interest for digital criminology. Their core concept to understand intelligence is surveillance (see Surveillance by Lyon), underscoring its connection to knowledge and power, defining it as "mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning threats and opportunities" (Gill and Phythian, 2018: 5). Though secrecy often characterizes intelligence activities and operations, the term 'mainly secret' also includes open and unclassified intelligence (Rønn, 2016). Intelligence can thus be understood as an organizational activity and a power process, where policies and actions enhance security and power relations by identifying what is believed soon to happen in the absence of countermeasures. As the availability of information is key to intelligence practices, digitalization creates a notable impact: it enables the collection, storage, and analysis of vast amounts of data. The possibility for precautionary types of intelligence has there-

fore increased tremendously, due to digitization of incidents, the accessibility of digital data, and big data analytics (Big Data by Završnik).

Framing intelligence

Within the scholarly tradition of international relations, intelligence is understood as mainly related to politics. However, particularly for criminology, intelligence is also about the making of 'crime intelligence' as part of police decision-making processes, touching upon tensions between knowledge, scientization, and politicization. Liberal democracies strive for a balance between intelligence measures and democratic values (Hillebrand, 2014: 305). Normative and ethical questions are paramount to research on intelligence, as its aims and measures are often unregulated by law (Rønn, 2016). As intelligence products lay the basis of intrusive interventions, ethical questions of trust, legitimacy, and democratic control are also crucial questions for researchers and practitioners (Diderichsen, 2016). Since the core element of intelligence is monitoring and surveillance, oversight bodies are important to ensure legitimacy.

The digital aspect of intelligence is central in the practices of information gathering and processing. Ratcliffe (2016 states that technology and intelligence-led policing are closely related, and Sheptycki shows how new information and communication technologies (ICT) fueled "the rise of 'intelligence-led policing'" (Sheptycki, 2004: 307). The information revolution of the 1990s reconfigured the police sector to take advantage of ICT, bringing intelligence and policing closer together. This 're-tooling' culminated in the introduction of various models of intelligence-led policing to improve the police's ability to collect, analyze, and disseminate crime intelligence. As intelligence practices require collection and use of data, understanding the role of digital technologies, such as sources, storage, and tools for analysis, is crucial to understand intelligence today. Before returning to these digital aspects of intelligence production in more detail, we present four ways of framing intelligence: As *a process*, *a product*, *a managerial effort*, and as *practice.* As we will show, all these approaches actualize intelligence in relation to digitalization.

The intelligence cycle is the most traditional model to conceptualize the *intelligence process* (Gill and Phythian, 2018). It presents a structured process, which in its simplest form comprise five stages: 1) planning and direction, 2) collecting, 3) processing, 4), analyzing, and 5) dissemination. According to Warner (2013), this structure came from French revolutionaries, who needed a means to explain intelligence collection to their increasingly specialized military staff. He asserts that the graphic depiction of a cycle became popular, even as governments moved beyond such a simple and linear process (Warner, 2013). The accuracy and relevance of this model has been critiqued for its simplification but is still commonly used. In line with the intelligence cycle, intelligence is often presented as the result of finding and turning data into information, which becomes intelligence when analyzed (Ratcliffe, 2016). This evolution from data to information has been challenged (Kaufmann, 2023), since data, too,

is information. Thus, data are treated in this contribution as a type of information. Bits of data are collected, and registered into various computer systems, quantified, processed, and analyzed using software before being disseminated. This datafication of intelligence (Chan et al., 2022) points to how data encoded in the intelligence system must be accounted for. With digitization, data is rendered digital and, hence, traceable. This datafication implies a process where "human actions are turned into data, often for strategic, optimization or governance purposes" (Flyverbom, 2022: 4). During such processes data is further constructed, translated, curated, and co-produced in dynamic interaction between humans and technologies, such as computer software and apps (Kaufmann et al., 2018; Lundgaard and Gundhus, 2024). This brings us to intelligence as a product.

The intelligence product is a means to an end. Its objective is to provide support for decisions on resource allocations and countermeasures. Ratcliffe (2016) defines intelligence as actionable knowledge for police managers. It is in this context the future oriented and proactive aspect of intelligence is rendered significant, underscored by terms such as 'probability' or 'likelihood.' The implementation of intelligence has been presented in terms of its scientific approach to crime analysis, though these claims of objectivity have been criticized (Vestby, 2018). Innes et al. (2005: 39) argue that the products should be recognized "as an artefact of the data and methods used in their construction, rather than providing an accurate representation of any crime problems," stating that the best intelligence products can do is to help reduce uncertainty. However, when intelligence products are disseminated, uncertainty or ambiguity is often less visible, as is any lack of essential data. Thus, the intelligence product, the basis for decision-making, may appear more certain than it is. Digitalization is also an aspect of this, as Bennett Moses and Chan (2018: 818) argue: "there is a potential accountability gap whenever the software itself becomes an acceptable basis for decision-making so that those to whom account is given do not (or are unable to) dig deeper." Intelligence, then, is the co-product of both humans and technologies, and decision-making ends up being partially outsourced to the software itself (Kaufmann, 2018).

Intelligence is also a managerial effort, and a way of governing knowledge production, as the product should be actionable and have a purpose. The implementation of intelligence-led policing was related to demands for cost efficiency, as well as for an increased focus on risk, control cultures, and securitization of social problems in the penal state (Garland, 2001). To apply scientific measures to manage and control crime was connected not only to a more scientific rationale (Innes et al., 2005), but also to managerialism and new public management. Risk-oriented institutional logics and risk assessments were also implemented in the private sector, and intelligence-led policing emerged in the 1990s at the intersection of science discourses, rationalization, and managerialism. Ericson and Haggerty (1997), as well as Innes and Sheptycki (2004) explored these new criminological fields as an issue of science and technology studies, highlighting the importance of technologies at this intersection, and arguing that such policing applies scientific concepts as a legitimizing aura of objectivity (see also Innes et al, 2005).

Intelligence as practice has been less researched than the aims, ideals, and knowledge products from intelligence. Thus, there is less research on how intelligence practices actually identify what may happen in the absence of any countermeasures. There is research on failures (see Gill and Phythian, 2018), but fewer studies on the ways in which intelligence-led policing is played out (Ratcliffe, 2016). What do the agencies do, and how do they do it? How are their practices enacted, and how do they influence intelligence at large? When looking into the practices of intelligence, it also becomes clear that there is a lot more happening than just core activities, such as collection, analysis, counterintelligence, and covert action. Much research "neglect the variety of activities that intelligence services have also engaged in, such as conducting diplomacy, guarding borders, running prisons, operating military units, designing atomic bombs, and managing professional soccer teams" (Stout and Warner, 2018: 517). Intelligence practices also have a digital dimension, as the digital systems used by intelligence agents and agencies have various affordances (Adams and Thompson, 2016), which shape and define the interactions between the technologies and the humans using them (boyd, 2011), and thus also the outcome of these interactions. The dependencies of technologies have been explored in implementation studies in the UK (James, 2013), Australia, Canada, New Zealand (Burcher and Whelan, 2019; Sanders et al., 2015; Weston, Bennett-Moses, and Sanders, 2019), Norway (Gundhus, 2013; Gundhus et al., 2022), and the US (Carter, 2013). Practices are not only reflecting human activities, but also those of the computational systems used as sources and for processing data and making intelligence products. Data systems can for example feature feedback loops, resulting in proactive policing that effects conceptions of crime conducted by people in the communities (O'Neil, 2016).

Control of political behavior to protect the state, what Brodeur (1983) calls *high policing*, relies on the storage of intelligence data. Since *low policing*, that is "routine law enforcement and street level order maintenance" (Reiner, 1985: 2), also increasingly includes intelligence methods, the need for digitization, data collection, and surveillance in day-to-day ordinary police work increases. The dilemmas posed by digitization thus mean that the increased use of high policing methods on low policing targets can impact trust and legitimacy due to a lack of accountability and oversight mechanisms (Bowling et al., 2019: 24; Brodeur, 2010).

Intelligence and digitalization

The use of intelligence in criminal justice systems speaks to broader *trends in criminal policies and practices*, such as pre-crime, prediction, and preemption, in combination with data-driven policing using various digital tools and software (McCulloch and Wilson, 2016). Data-driven approaches to information reinforce a larger trend towards the "management of visibilities," where only coded data can be used and considered a valid knowledge base (Flyverbom, 2022).

Digitalization makes intelligence an intriguing field for criminologists interested in the production and use of knowledge by states, in law enforcement, or elsewhere. Digitalization enables an increased sharing of information and is implemented in view of changing the working practices of the organizations (Chan et al., 2022). Ratcliffe claims such change is a necessary step in policing, as knowledge "must be structured in a way that can help decision-makers develop policy" (Ratcliffe, 2016: 74). Due to the explosion of openly available information (so-called OSINT), much intelligence is now taking place online, where the collection of data is often seen as low in risk and high in reward (Clemente, 2014). The availability of recorded data enables new strategies for knowledge production, while established knowledge production changes through access to new software for data integration.

Techniques for analysis change due to new software, machine learning, and language models. Such developments in software products support the move towards more surveillant policing (Brayne, 2020) and can challenge police legitimacy, as the use of predictive software may undermine the ability of individual officers or police authorities to account for their decisions (Bennett Moses and Chan, 2018). Digitalization could also create more self-fulfilling prophecies, as problems and harmful situations may arise as police bodies act against predicted futures (Bowling et al., 2019: 33, see also Fyfe et al., 2018). Thus, digitization changes intelligence, and has also extended the powers of the police.

Conclusion

Intelligence is an elusive and dynamic concept. Intelligence-led policing emerged in the context of supporting traditional investigative police-led strategies and specialist police operations but is now increasingly framed as a process model used to underpin the managerial organizational structures designed to improve future police work. Intelligence represents a certain type of *actionable* knowledge about a specific criminal environment, intended to inform and reduce uncertainties for decision-makers (Fyfe et al., 2018). For criminology it is essential to understand and explore what becomes the focus of intelligence when intelligence issues are related to crime, deviance, and risk. New trends in risk and crime control can influence intelligence practices, as can the development of digital technologies. Developments in intelligence are closely linked to technological advancements, as they provide new ways of collecting, storing, analyzing, and presenting data and information. These advancements also link intelligence analysis to other digital technologies, such as prediction technologies and other data integration platforms (see Platforms by Egbert).

Main takeaways

- Intelligence is an elusive concept but has a long history in both governmental and non-governmental organizations aiming at 'knowing the enemy,' often using secret methods.
- Intelligence can be understood both as a process, a product, a managerial concept, and as a practice.
- Intelligence is not neutral and objective but reflects the political context it works within.
- Digitalization has opened for new ways of collecting, storing, processing, and sharing intelligence.
- *Who* and *what* is defined as a threat and risk emerge from intelligence practices and is influenced by the digital tools and systems used throughout the process.

Suggested reading

Fyfe, N. R., Gundhus, H. I., & Rønn, K. V. (2018). *Moral Issues in Intelligence-led Policing.* London: Routledge.

Gill, P., & Phythian, M. (2018). *Intelligence in an Insecure World* (3rd ed.). Cambridge: Polity Press.

Ratcliffe, J. H. (2016). *Intelligence-led Policing* (2nd ed.). London: Routledge.

Sanders C. B., Weston, C., & Schott, N. (2015). Police innovations, 'secret squirrels' and accountability: Empirically studying intelligence-led policing in Canada. *British Journal of Criminology*, 55(4), 711 – 729.

Sheptycki J. (2017). The police intelligence division-of-labour. *Policing and Society*, 27(6), 620 – 635.

References

Adams, C., & Thompson, T. L. (2016). *Researching a Posthuman World: Interviews with Digital Objects.* London: Palgrave Macmillan. https://doi.org/10.1057/978-1-137-57162-5.

Bennett Moses, L., & Chan J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. *Policing & Society,* 28(7), 806 – 822. https://doi.org/10.1080/10439463.2016.1253695

Bowling, B., Reiner, R., & Sheptycki, J. (2019). *The Politics of the Police* (5th ed.). Oxford: Oxford University Press. https://doi.org/10.1093/he/9780198769255.001.0001

boyd, d. (2011). Social network sites as networked publics. Affordances, dynamics, and implications. In Z. Papacharissi (ed.), *A Networked Self: Identity, Community, and Culture on Social Network Sites* (pp. 39 – 58). New York: Routledge.

Brayne, S. (2020). *Predict and Surveil. Data, Discretion, and the Future of Policing.* Oxford: Oxford University Press.

Brodeur, J.-P. (1983). High and low policing: Remarks about the political activities. *Social Problems*, 30(5), 507 – 520.

Brodeur, J.-P. (2010). *The Policing Web.* Oxford: Oxford University Press.

Buckley, J. (2013). *Managing Intelligence: A Guide for Law Enforcement Professionals.* New York: CRC Press. https://doi.org/10.1201/b15515

Burcher, M., & Whelan, C. (2019). Intelligence-led policing in practice: Reflections from intelligence analysts. *Police Quarterly*, 22(2), 139 – 160. https://doi.org/10.1177/1098611118796890

Carter, J. G. (2013). *Intelligence-led Policing: A Policing Innovation.* El Paso: LFB Scholarly.

Chan, J., Sanders, C., Bennett Moses, L., & Blackmore, H. (2022). Datafication and the practice of intelligence production. *Big Data & Society*, 9(1). https://doi.org/10.1177/20539517221089310

Clemente, D. (2014). Cybersecurity. In R. Dover, M. Goodman, & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies* (pp. 256 – 263). London: Routledge.

Diderichsen, A. (2016). Om efterretningstjenesters legitimitet. In K. V. Rønn (ed.), *Efterretningsstudier* (pp. 67 – 88). Frederiksberg: Samfundslitteratur.

Ellefsen, B., & Lomell, H. M. (2024). Polisiær etterretning i et historisk perspektiv. In E. B. Unneberg, P. Jansen, & O. Trønnes (eds.), *Etterretningsanalyse i politiet* (pp. 36 – 56). Oslo: Universitetsforlaget.

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the Risk Society.* Oxford: Clarendon Press. https://doi.org/10.3138/9781442678590

Flyverbom, M. (2022). Overlit: Digital architectures of visibility. *Organization Theory*, 3(3). https://doi.org/10.1177/26317877221090314

Fyfe, N. R., Gundhus, H. I., & Vrist Rønn, K. (2018). *Moral Issues in Intelligence-led Policing.* London: Routledge.

Garland, D. (2001). *The Culture of Control.* Oxford: Oxford University Press.

Gill, P., & Phythian, M. (2018). *Intelligence in an Insecure World* (3rd ed.). Cambridge: Polity Press. https://doi.org/10.1111/1478-9302.12073_52

Gundhus, H. I. (2013). Experience or lnowledge? Perspectives on new knowledge regimes and control of police professionalism. *Policing: A Journal of Policy and Practice*, 7, 176 – 192.

Gundhus, H. O. I., Talberg, N., & Wathne, C. T. (2022). From discretion to standardization: Digitalization of the police organization. *International Journal of Police Science & Management*, 24(1), 27 – 41. https://doi.org/10.1177/14613557211036554

Hillebrand, C. (2014). Intelligence oversight and accountability. In R. Dover, M. Goodman, & C. Hillebrand (eds.), *Routledge Companion to Intelligence Studies* (pp. 305 – 312). London: Routledge.

Innes, M., & Sheptycki J. (2004). From detection to disruption: Intelligence and the changing logic of police crime control in the United Kingdom. *International Criminal Justice Review*, 14(1), 1 – 24. https://doi.org/10.1177/105756770401400101

Innes, M., Fielding, N., & Cope, N. (2005). 'The appliance of science?': The theory and practice of crime intelligence analysis. *The British Journal of Criminology*, 45(1), 39 – 57. https://doi.org/10.1093/bjc/azh053

James, A. (2013). *Examining Intelligence-Led Policing. Developments in Research, Policy and Practice.* Basingstoke: Palgrave Macmillan.

Kaufmann, M. (2023). *Making Information Matter: Understanding Surveillance and Making a Difference.* Bristol: Bristol University Press.

Kaufmann, M., Egbert, S., & Leese, M. (2018). Predictive policing and the politics of patterns. *The British Journal of Criminology*, 59(3), 674 – 692. https://doi.org/10.1093/bjc/azy060

Kent, S. (1966). *Strategic Intelligence for American World Policy.* Princeton: Princeton University Press.

Lundgaard, J. M., & H. O. I. Gundhus (2024). Den digitale hviskeleken: Data, informasjon og kunnskap i etterretningsstyrt politiarbeid. In E. B. Unneberg, P. Jansen & O. Trønnes (eds.), *Etterretningsanalyse i politiet* (pp. 220 – 232). Oslo: Universitetsforlaget.

McCulloch, J., & Wilson, D. (2016). *Pre-crime. Pre-emption, Precaution and the Future.* Abingdon: Routledge.

O'Neil, C. (2016). *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy.* New York: Crown.

Ratcliffe, J. H. (2016). *Intelligence-led Policing* (2nd ed.). London: Routledge. https://doi.org/10.4324/9781315717579

Reiner, R. (1985). *The Politics of the Police.* Brighton: Harvester Wheatsheaf.

Rønn, K. V. (2016). Efterretningsetik udenfor lovens rammer. In K. V. Rønn (ed.), *Efterretningsstudier* (pp. 219 – 246). Frederiksberg: Samfundslitteratur.

Sanders C. B., Weston C., & Schott N. (2015). Police innovations, 'secret squirrels' and accountability: Empirically studying intelligence-led policing in Canada. *British Journal of Criminology*, 55(4), 711 – 729.

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology*, 1(3), 307 – 332. https://doi.org/10.1177/1477370804044005

Stout, M., & Warner, M. (2018). Intelligence is as intelligence does. *Intelligence and National Security*, *33*(4), 517 – 526. https://doi.org/10.1080/02684527.2018.1452593

Vestby, A. (2018). Policy-making without politics. Overstating objectivity in intelligence-led policing. In N. R. Fyfe, H. O. I. Gundhus, & K. V. Rønn (eds.), *Moral Issues in Intelligence-led Policing* (pp. 265 – 282). Routledge. https://doi.org/10.4324/9781315231259-14

Warner, M. (2013). The past and future of the Intelligence Cycle. In M. Phythian (ed.), *Understanding the Intelligence Cycle* (pp. 9 – 20). London: Routledge.

Weston, C., Bennett-Moses, L., & Sanders, C. (2019). The changing role of the law enforcement analyst: Clarifying core competencies for analysts and supervisors through empirical research. *Policing and Society*, 30(5), 532 – 547. https://doi.org/10.1080/10439463.2018.1564751