Policing & Society, Vol. 16, No. 1, March 2006, pp. 7–26

Routledge
Taylor & Francis Group

Knowledge Workers or "Knowledge" Workers?

Jean-Paul Brodeur & Benoît Dupont

This paper focuses on the role of knowledge in policing and questions the application of the notion of network to describe police organizations in themselves or in relationship with each other. First, the concepts of knowledge and of network are critically assessed for their own. Second, their applicability to policing is examined in respect to criminal investigation, the handling of police informants, high (or political) policing, and counterterrorism. This examination is conducted with a particular emphasis on information reliability and overload. It is concluded that while it is premature to argue that focusing on knowledge and networks has generated a paradigm shift in respect to policing, both concepts may have the potential to generate a new paradigm.

Keywords: Information; Knowledge; Network; Investigation; Informants; Counterterrorism; Information sharing; Information reliability; Information overload

There have been at least two significant developments in the theory of policing in the last 10 years. The first is the growing importance of a cluster of concepts that stem from the core notion of *information*, such as meaning, intelligence, knowledge, information technology, and data mining. Seeing the police as "knowledge workers" is a result of this development (Ericson & Haggerty, 1997), which is scrutinized many researchers (de Lint, 2003). A second development, not yet as influential, is the introduction of the notion of network to reflect the fact that policing involves many participants (Johnston & Shearing, 2003; see also Bayley & Shearing, 2001). These developments are not, of course, specific to the theory of policing but reflect wider changes within social theory, such as concern about the "knowledge society" (Böhme & Stehr, 1986; Ericson et al., 1987) and the "network society" (Castells, 1996). They have also generated changes in the practice of policing, such as the creation of

Correspondence to: CICC, Université de Montréal, Cop. 6128, Succ. Centre-Ville, Montréal, Québec, H3C 3J7, Canada. Jean-Paul Brodeur and Benoît Dupont are both researchers at the International Centre for Comparative Criminology.

ISSN 1043-9463 (print)/ISSN 1477-2728 (online) © 2006 Taylor & Francis
DOI: 10.1080/10439460500399304

intelligence-led policing and the outsourcing of large chunks of policing to private partners ("lateralisation"). While discussing both these developments, we will focus more on the role of knowledge in policing than on the place of networks.

The concepts of knowledge and networks were introduced to the sociology of policing without clear definition of which part of policing they were most applicable to. It was said either that they were relevant to policing in general or to the most visible part of police organizations, the activity of the uniformed police. Rather than pursuing these general statements, we assess the role of knowledge with respect to those aspects of policing that are the most germane to information or knowledge work. The paper is thus divided into four parts. We begin with a theoretical discussion of the concept of knowledge and some of its variants (e.g. "intelligence"). This is followed by examination of the role of knowledge and networks in the fields of criminal investigation, in the handling of police informants, and in high or political policing, particularly in the field of counter-terrorism (for a discussion of high policing, see Brodeur, 1983, 2005; also see Brodeur and Leman-Langlois, 2006, forthcoming).

Our perspective can be best defined through the brief discussion of one example. Saying "I *believe* that there are Americans camping on the hidden side of the moon, but then I may be wrong" carries no contradiction, because one can believe something that is false. As Bertrand Russell stressed a long time ago, belief statements are not truth functional. However, saying "I *know* that there are Americans camping on the hidden side of the moon, but then I may be wrong" entails a contradiction: one cannot claim at the same time to know something and to be in doubt. How do we figure this difference between the expression of belief and of knowledge? There is a tradition stemming from Wittgenstein's *Philosophical Investigations* (1953) and leading to Searle's *Speech Acts* (1969) that belongs to logic, semantics and, more generally, to analytical philosophy. It tries to answer Wittgenstein's call to resist the "craving for generality" and not to fail distinguishing what are the different ways to use language. The expression of belief, information and knowledge are all very different speech acts. The purpose of this paper is to show how much they are different within the context of security intelligence. The same discriminant analysis is applied to the notion of network.

The Concepts of Knowledge and of Network

Knowledge

In their influential book, Ericson and Haggerty offered "a fundamental reassessment of how we think about the police" (1997: 3). They proposed that policing be seen as risk communication (1997: 3), the police as "knowledge workers" (1997: 19), and community policing as "communications policing" (1997: 70; part 5 of their work is devoted to how knowledge is communicated rather than to its production). Ericson and Haggerty do not provide an explicit discussion of the meaning of such key concepts as knowledge, communication, and information (the first two are not even listed in the book's index). We eventually learn that knowledge is "that which is objectified in institutional representations, a property and resource that provides a capacity for action" and that no distinction is made between information and knowledge (1997: 83–84).

Ericson's emphasis on the role of information/knowledge goes all the way back to his first book, *Making Crime* (1981), where he correctly emphasized that the work of detectives is driven by information. He had actually begun to refer to the *knowledge society* as such at least 10 years before *Policing the Risk Society* (1997), in the first book of his trilogy on policing and the media (Ericson et al., 1987: 11), where he considered journalistic news to be a kind of knowledge. His view of knowledge ("the belief that something is real" and "the objectivated meanings of institutional activity" (Ericson et al., 1987: 11) was taken from the classic work of Berger and Luckmann (1966) on the sociology of knowledge. This latter work is quoted at the beginning of Ericson and Shearing's paper (1986) on the "scientification" of police work and its influence on Ericson's thought is obvious.

Berger and Luckmann have left their unmistakable imprint on the sociology of knowledge through their emphasis on the idea that the sociology of knowledge must concern itself with everything "that *passes* for 'knowledge' in society" (1966: 13, our emphasis, quotation marks in text). The momentous change introduced by their perspective is that knowledge is now defined through a subjective attitude ("the certainty that phenomena are real") rather than as an external validity, as it is current in science (Berger & Luckmann, 1966: 1). The epistemological and methodological problems that were a major concern of the originators of the sociology of knowledge are thus no longer part of the discussion (Berger & Luckmann, 1966: 12). Berger and Luckmann have been followed in this by Ericson, who asserts, "knowledge is not a matter of true belief but of whatever people take to be knowledge, regardless of validity" (Ericson et al., 1987: 11). The idea that knowledge is "any and every set of ideas and acts" that is pertinent to what a social group accepts as real is now firmly ensconced in the field of the sociology of knowledge (McCarthy, 1996: 23). There is, however, one caveat to the extension of the use of the word knowledge, explicitly formulated by Berger and Luckmann, that deserves to be quoted. After introducing the key terms "reality" and "knowledge" in their basic theoretical discussions they add:

> If we were going to be meticulous in the ensuing argument, we would put quotation marks around the two afore-mentioned terms every time we used them, but this would be stylistically awkward. (Berger & Luckmann, 1966: 1–2)

The sociology of knowledge was quick to dismiss this caveat and *knowledge* was substituted for "knowledge" without further explanation. Nevertheless, there is a crucial difference between developing a sociology of *knowledge* and a sociology of "knowledge": the quotation marks indicate that the word knowledge is not to be taken in its current sense of validated information—*genuine* knowledge as opposed to what *passes* for it—and that social *psychology* is being substituted for epistemology (Berger & Luckmann, 1966: v). Explaining this difference would require examination of complex epistemological issues. For instance, the definition of knowledge offered by Berger and Luckmann conflates faith and knowledge, putting both under the heading of belief in something held to be real, thus contradicting one of the strongest traditions of philosophy. However, we shall avoid these deeper philosophical concerns and limit ourselves to raising four issues that are particularly relevant to a theory of policing.

Oversimplification

The title of Berger and Luckmann's (1966) treatise in the sociology of knowledge is *The Social Construction of Reality*. The defining question for such an undertaking is "how is it possible that human activity should produce a world of things" (Berger & Luckmann, 1966: 17). Being a process, knowledge is considered to be the main reality-producing force, superseding the less dynamic notion of information. The sociology of knowledge thus becomes a study of the *effect* of our certainty that phenomena are real on what we define as factual and on our behaviour in relation to these facts. Berger and Luckmann do not, however, examine the specific ways in which we reach this certainty. How the faithful come to believe in their God, the scientist in his equations, or the police in the guilt of a suspect is taken for granted and seems to stem from some foundation in "everyday life" (Berger & Luckmann, 1966: part 1). This appears to us to oversimplify the issue of certainty and, to the extent, the issue of knowledge. What matters for them is not how we reach certainty about what is real but how we act after having reached this (unaccounted for) certainty. As Berger and Luckmann make clear, epistemology is excluded from the sociology of knowledge. A theory of action based on this understanding cannot easily differentiate between descriptions and predictions, as both qualify equally as actionable knowledge. However, treating specific factual statements ("The Twin Towers collapsed on September 11, 2001") and indeterminate predictions ("A group linked to Al Qaeda is planning a massive strike against the US at some point in the future") as of equal importance to the field of intelligence would certainly undermine attempts to articulate definite counter-strategies.

Validation

Validation is to "objective facticities" what certainty is to "subjective meanings" (Berger & Luckmann, 1966: 17). Theories of the objective validation of knowledge belong to the fields of epistemology and methodology, which are explicitly excluded from the sociology of knowledge. Is there a problem with allowing the sociology of knowledge to define its perspective as it sees fit and thus to exclude validation, which it seems to consider irrelevant? It depends on what kind of knowledge we focus on. In everyday life, whether we consider some phenomena to be real may have limited consequences. However, what the police consider to be knowledge is used to shape actions that are traditionally focused on coercion and may cause lethal harm. For instance, it may be decided that members of a minority group should be confined in concentration camps because they are believed to be a “clear and present danger” or that a country should be invaded on the basis of intelligence that indicates a threat. Racial prejudice is an overwhelming belief in the reality of racial inferiority. According to us, it cannot be referred to as knowledge without demeaning the sense of the word: a theory allowing that racial prejudice be referred to as “knowledge” or what passes for it has got to be flawed. A horse with a hunchback might pass for a camel, but it won’t make it through the desert. Side-stepping the whole issue of validating one’s information by declaring it equivalent to knowledge or failing to question one’s certainties because they seem convincing may lead to grievous consequences and can be considered morally irresponsible. When it is divorced from epistemology, as it is in Berger and Luckmann, the sociology of knowledge is a descriptive undertaking and has little to contribute to the methodology of science *per se*. Epistemology and methodology have a prescriptive aspect and can be used to increase the validity of knowledge and intelligence used in policing. In a stimulating paper, Innes et al. (2005) rediscovered the relevance of “applying an epistemologically oriented critique of some of the key techniques associated with crime analysis”.

Secrecy

It is surprising that this issue has not yet received the attention it deserves: indeed, not all knowledge can be publicly disseminated. Policing requires a certain amount of secrecy. The amount of secrecy required increases drastically as we move from the most visible part of policing—uniformed patrol—to the least conspicuous—criminal investigation, surveillance, and the protection of national security, the latter being almost wholly shrouded in secrecy and kept from public “knowledge”. Furthermore, policing considered as risk communications is extremely vulnerable to political interference, as was seen in the way colours were opportunistically used at times to indicate an increase in the level of the risk of terrorism, for the purpose of manipulating public opinion in the US.

Trust

Considered subjectively, knowledge is information that can be trusted. It should be said that the subjective side of knowledge is not the corner-stone of its definition, which rests on objective validation (to the extent that it can be achieved).[1] However, in certain fields of policing, such as the collection of human intelligence, the issue of whether informants can be trusted forces police handlers to draw hard distinctions between information, disinformation, and potentially genuine knowledge, these distinctions being reflected in police language. Acting on information, evidence or knowledge is seen as different. Furthermore, equating information and knowledge avoids the whole issue of trust, which is vital in the field of policing (Manning, 2003).

Networks

While there are several issues that could be raised regarding the application of the notion of networks to policing, we mention only one of them. The word "network" is used in the field of police studies either metaphorically (usually unintentionally) or, more frequently, as a notion that is based on intuition, not on the stimulating research that is available about networks (Burt, 1992, 2004; Castells, 1996; Morselli, 2001, 2003). Often, little distinction is made between a transnational network of policing organizations (Bigo, 1996) and a national formal or informal network of police. The latter can take several forms: a cluster, a clique, a hierarchy or finally a network in its proper sense (see Burt, 1992; United Nations Centre for International Crime Prevention, 2000). To these we may add computer networks that support communication within institutional and social structures (Dupont, 2004). Inexact use of the term network evokes notions of highly coordinated assemblages, by analogy with communications or transport networks, while the reality is more complex and ambiguous. For example, networks (in the sociological sense of the term) can be identified within groups of people or organizations where there is no explicit awareness of the numerous and indirect links that make up such networks.

The concepts of knowledge and, to a lesser extent, networks are laden with history, highly structured, and have an inner complexity that cannot be eliminated by putting them within quotations marks—especially when these are later erased. Ignoring these features not only leads to misunderstandings but also hinders exploration of the insight that, in an increasing number of aspects of their work, the police may be operating as information managers.

Policing and Criminal Investigation

It is not immediately apparent that police activity can be considered knowledge work. The most influential definition of policing characterizes it as a mechanism for the distribution of coercive force according to an *intuitive grasp* of situational exigencies (Bittner, 1990: 131).[2] This stress on quick thinking in emergency situations suggests that policing is a profession dedicated to action rather than to reflection, an observation reflected in both teaching and in fieldwork.

The impressive multiplication of the number of forms that the police have to fill out may be indicative of a scientification of police work, if we only consider the blank forms. When, however, we look at how the forms are actually filled out by police officers (with very little zeal), it indicates instead a stifling bureaucratization of policing—a trend which is acutely resented. In criminal intelligence seminars we have organized, a common complaint by the police who lead such intelligence units is that management tends to staff them with lower performing officers because knowledge work ("shuffling paper") is little valued and carries no prestige within the organization.[3] Even the basic task of creating reports to keep the public informed about police efforts is seen as of very little value, as shown in a study one of us conducted of the unsuccessful efforts of the Québec (Canada) department of public security to persuade the province's police forces to issue an annual report that provided very basic information about their operations (Cayouette & Brodeur, 2004).

The word "investigation" is inescapably associated with knowledge work and can be found in the title of many theoretical works (e.g. Wittgenstein's *Philosophical Investigations*, 1953). The investigation of crime would thus seem an ideal field in which to study police knowledge skills at work. One of us (Brodeur) conducted research in the CID files of a major police force in Québec. A sample of cleared cases where suspects had been prosecuted was collected for the years 1990–2001. Originally 125 cases involving drug trafficking, fraud, sexual assault, robbery and homicide were collected. Records for homicide investigations were, by far, the most extensive and a larger sample of 153 homicide cases involving 191 suspects was collected, coded according to a breakdown of 163 variables, and quantitatively analysed. The results of the statistical analyses were used to conduct in-depth interviews with homicide investigators, which provided strong confirmation of the quantitative findings. Among the most general findings were:[4]

- In 80 per cent of cases, the suspect who will eventually be prosecuted is identified within 24 hours or less (in 53 per cent of cleared cases, the suspects were identified immediately by police answering a 9–11 call). In 68 per cent of the cases identified suspects were arrested within 24 hours. (In 44 per cent of these cases arrest coincided with identification and was immediate).
- Key factors leading to the identification of suspects charged with homicide were the testimony of an eye witness still present at the crime scene (22.5 per cent of cases), spontaneous confession by the suspect (20.5 per cent), and denunciations by various people (police informant, accomplice, friend, family member or spouse (30 per cent). In other words, in almost all homicide cases the police are able to identify a suspect because someone tells them who he or she is. Investigative work, electronic surveillance, forensics, and intelligence are of marginal importance and were significant in less than 2 per cent of the cases.
- Key factors in the arrest of an identified suspect closely parallel the findings for identification: patrolmen and women arrest 23.5 per cent of suspects in *flagrante delicto* and suspects give themselves up in an additional 20 per cent of cases. Criminal investigation and other factors listed above play a marginal role here as well.
- The use of forensics and all types of expertise (DNA, polygraph, hypnosis) were also examined. One of these factors was determinant of the outcome of a case in

less than 3 per cent of the cases, with the exception of the polygraph, which essentially serves to eliminate potential suspects.

- There was no indication that private security played any role in clearing homicide cases.

These results are in line with the research literature. Although his UK sample was limited (20 cases), Martin Innes found that half the cases he examined were "self-solvers" (Innes, 2003: 292). Recent research conducted in the US of a sample of 589 cleared homicide cases found that the key determinant for solving a case was information provided by eyewitnesses and other informants (60.5 per cent of cases; Wellford & Cronin, 1999: Table 9, p. 27). They also found that half the homicide cases in their sample were solved in less than a week. The importance of police patrols in solving criminal cases was recognized by Richard V. Ericson in his study of general crime investigations (1981, 136). He characterized the role of investigators as limited to processing suspects already made available by the patrol officer.

One of the implications of these findings with regard to the role of knowledge work in criminal investigation creates a paradox. In the great majority of cases, not only are murder cases resolved too quickly to require any significant amount of knowledge work but cases are self-resolving. In cases where there is sufficient time for knowledge work, there is a strong probability that the investigation will end in failure, as cases are usually cleared quickly or not at all. Perhaps we need to make a distinction between a theory of how murder cases are cleared and a theory of homicide investigation. Only the latter would involve knowledge work understood in more than its minimal sense, the extent of such knowledge work being paradoxically proportional to the degree of its probability to end in failure. This finding vindicates Greenwood's controversial conclusion that halving the time devoted by investigators to their inquiries would make no difference in clearance rates (Greenwood et al., 1977).

The Handling of Police Informants

Collecting human intelligence (HUMINT) is vital to policing operations. As the Pentagon realized in its fight against terrorism, signal intelligence (SIGINT) provided by technology is no substitute for HUMINT (Schmitt, 2005). The handling of informants is as much a part of criminal investigation as investigation. Limiting our discussion to criminal intelligence, we raise three issues with respect to the handling of police informants. In discussing these issues, we draw a distinction between two kinds of police informants, *delators* and *informers*. Delators are informants who appear in court to testify for the prosecution (a "protected witness" in the US or a "supergrass" in Northern Ireland). Informers are police sources who do not as a rule appear in court, allowing them to continue to provide the police with information on criminal circles. Following the spectacular success of use of "*pentiti*" (repentant terrorist or *mafiosi*) in Italy, there is now a trend in democratic countries to enshrine in law the use of delators.

Secrecy

The identity of police and security services sources is one of the most closely guarded secrets of policing. In Canada, police informers have been granted unconditional protection[5] of their identity by two rulings of the Supreme Court (*Solicitor General of Ontario* v. *Royal Commission of Inquiry*), [1981] and *Bisaillon* v. *Keable*, [1983]). This protection is almost limitless, as it extends to whatever might lead to the identification of a police informant. (As information that could be provided only by one informer is a clue to his or her identity, protection of an informer's identity covers the content of what he or she told police.) Security services hold to a strict interpretation of informer protection and strongly object to their sources appearing as public witnesses in court proceedings. This is the root of the so-called "wall" between police and security services and the latter's condemnation of the police "tyranny of the case file", which dictates that all cases must end in public court proceedings (Shelby, 2002: 62). The existence of this wall was also acknowledged in Canada when the two defendants in the Royal Canadian Mounted Police (RCMP) case against the perpetrators of the 1985 Air India bombing (329 victims) were acquitted on 16 March 2005, after a police investigation that lasted for 20 years and cost CAN$ 130 million. The Canadian Security Intelligence Service (CSIS) is on record for having erased electronic surveillance tapes that might have identified a source if produced as evidence in a public trial. Our working hypotheses is that the existence of a wall between criminal and security intelligence will be found whenever police proceedings are thoroughly investigated, following a high profile failure of co-ordination. The crucial implication of secrecy—of which the protection of sources is only one aspect—is that obstacles to the sharing of information between the various policing organizations (including security services) cannot be seen as the result of police occupational culture alone. They are in significant part *legal* and cannot be eliminated merely by claiming that all police are legally entitled to share all policing information. This point is further discussed in the next part of this paper.

Trust

The issue of trust is best exemplified with respect to delators. Delators (protected witnesses, supergrasses) are paid for the information they provide and, most importantly, for their testimony in court. Benefits are the informal rule with police informants. With delators, this rule is made official through detailed contractual agreements. In Québec, professional delators have created a "syndicate" to represent them because they feel that the Department of Justice does not abide by its commitments to them. The wheeling and dealing that takes place with police delators is well known in Canada and has been extensively reported in the media. The resulting high profile of delators has led lawyers (and the media) to question whether these witnesses should be trusted in court, as they are paid to testify. The courts have grown increasingly distrustful of such testimony and no conviction can be secured by the prosecution on uncorroborated evidence provided by a delator. This distrust now affects all police and security services informers and an elaborate system for grading the trustworthiness of informers and for corroborating HUMINT of various origins has been developed (Canada, House of Commons, 1990: 109). To conclude, there is a crucial difference between information, disinformation and trusted intelligence (knowledge) in the field of HUMINT, with the question of validity being the central concern. These categories were integrated to official terminology by police agencies and security services and they are now used to assess and to classify HUMINT.

Compartmentalization

The previous issues of secrecy and trust come together to create the problem of intelligence compartmentalization, as shown in the following example. During the October Crisis of 1970—the greatest political crisis generated by terrorism in Canada—the Security Department of the RCMP intercepted a warning from a member of a Québec police force to one of their prime terrorist suspects.[6] This police force was immediately removed from any involvement with operations to resolve the crisis and was no longer given access to sensitive information. There has been much speculation over why this warning was given. One of the most current explanations among government investigators of the Crisis is that the terrorist was a valuable informer for the drug squad of the police force that issued the warning. Few examples as significant as this surface in public inquiries. First, it shows that relationships between policing organizations are decided on the basis of trust. Second, it indicates that the compartmentalization of intelligence affects not only the sharing of information between different policing agencies but also determines the behaviour of various units within the same policing organization. It cannot be assumed that what constitutes success is the same for different units.

Counterterrorism and the Enemy Within

Intelligence-led policing is, to an important extent, an offspring of problem-oriented policing, which emphasizes building a knowledge base for police operations. In past years, appending the qualifier “oriented” to a noun (“community”, “problem”) has been a way to mark the advent of a police strategy and police executives recently introduced the idea of “terror-oriented policing” to refer to the “new normal” in policing (Simonetti Rosen, 2004a). This new designation brings “intelligence” in “intelligence-led” policing closer to its original meaning in special interest policing and stresses the growing importance of national security, once the stronghold of security services, to policing.

In the realm of counterterrorism, the failure to convert information into knowledge can lead to catastrophic outcomes, as the dramatic events of 9/11 and 3/11 have shown. The figure of the Greek deity Proteus, who not only knew everything about the past and the present but could also foretell the future, epitomizes the ambition of counterterrorism units and high policing activities in general (L'Heuillet, 2001). However, Homer also describes how reluctant Proteus was to share his knowledge, granting this privilege only to those such as Menelaus who captured him through elaborate stratagems (Homer, 1919 [800BCE]: book 4). In this respect police and intelligence organizations are much like Menelaus, although they resort to computer systems rather than seal skins in order to get answers to their queries.

Information Overload

The quantity of data the police must deal with is overwhelming. In line with a general trend that sees an exponential growth in the quantity of information created and stored (Lyman & Varian, 2003), and anxious not to miss the details that would allow them to "connect the dots", analysts are inundated by a flow of data that ultimately interferes with the intelligence process. James Sheptycki's fieldwork in British criminal intelligence units reveals this very clearly. The situation has led intelligence practitioners to use such powerful metaphors "drinking from a fire-hose" (Sheptycki, 2004b: 317) or "boiling the ocean" (Griffin, cited in Singel, 2003). This bleak assessment of the capacity to differentiate "noise" from relevant information is unlikely to change, given current technological circumstances.

The website of ARDA (Advanced Research and Development Activity), the research and development program of the National Security Agency (NSA) and associated departments, states that some existing intelligence databases grow at the rate of four petabytes per month.[7] And the new US-Visit program, which will combine existing immigration databases and record personal information on the 54 million non-US residents who cross the border annually in order to screen for potential terrorists, is expected to collect several petabytes of data every year (Singel, 2003). A petabyte is the current largest metric designation of storage capacity in discrete computer systems. In layman's terms, a petabyte of data is equivalent to half of all the content of US academic research libraries or 50 times the Library of Congress holdings. Private databases maintained by "data aggregators" such as ChoicePoint, Seisint, Lexis-Nexis, or Acxiom, which contain hundreds of millions of customer profiles, contribute a few more petabytes of information as they are gradually made available to intelligence analysts (O'Harrow, 2005).

Most of this terrorism-related information, however, remains unusable until it has been processed. For example, telecommunication intercepts often need to be translated. The backlog revealed by the inspector general of the US Department of Justice is quite telling: his most recent audit of the FBI language services section suggests that, as of the first quarter of 2004, more than 123,000 hours of counterterrorism audio intercepts collected since 2002 had not been translated. Material collected by counterintelligence programs added more than 500,000 hours to that number. Overall, 30 per cent of potentially highly relevant information went unreviewed and had to be deleted from antiquated computer systems in order to free space for incoming data (Office of the Inspector General, 2004: ix). Similarly, no intelligence analyst can possibly make sense of the billions of transactions or travel itineraries that are systematically reported by financial institutions and airlines. This arduous task is instead delegated to datamining software and computer systems (designed by engineers, not police officers) that constantly monitor flows of data in search of suspicious patterns. This process of brute information management constitutes only the embryonic stage of knowledge work.

Sharing Information

There is a significant body of literature on the reluctance of policing organizations to share information and, more generally, on the organizational and technical obstacles to sharing information (Sheptycki, 2004a and b). After the 9/11 attacks, this topic became the major theme of numerous official reports on the failings of the intelligence community (National Commission on Terrorist Attacks Upon the United States (NCTAUS), 2004; Shelby, 2002). However the research literature and the official reports failed to fully acknowledge a major hurdle in the sharing of information: the *legal impediments* to breaching state secrecy. According to the US Information Security Oversight Office, in 1995 there were 21, 871 "original" Top Secret designations and 374,244 "derivative" designations. (Some two million government officials, in addition to one million industrial contractors, have "derivative classification" authority (US Congress, 1997: Chairman's Foreword, p. xxxix).) Many of these derivative designations are intended to protect the "sources and methods" of collecting national security intelligence. The classification of documents as secret (including the most mundane of policy papers) is notoriously overused by the current Bush administration. In Canada, as in the UK, official secrets legislation covers the field of "national security", very broadly defined, and makes it an offence for any person permanently bound to secrecy to communicate or confirm without authority "special operational information" to anyone for whom it is not officially intended.[8] The idea that all policing organizations are equally entitled to share classified information on the basis that they are all part of the police apparatus is a myth. The strictures of official secrecy apply as much to the police as to other organizations, particularly with respect to the sharing of information between local and central police agencies (local police, for instance, do not have any security clearance).

On the one hand, security intelligence agencies resist the "tyranny of the case file" (Shelby, 2002: 62) that compels undercover operatives to testify in public. On the other hand, law enforcement agencies resent the high-handedness of security services with respect to the legal constraints bearing on court proceedings. Police organizations are not academic learned societies designed for the purpose of sharing knowledge but government agencies that disseminate intelligence on the basis of the “need to know” principle—a principle that is determined as much by organizational and political imperatives as it is by the law. As was shown in a study on air transportation security recently released by the 9/11 Commission, the withholding of information is a process that feeds on itself: agencies justify their failure to transmit intelligence to their partners by claiming that they were ignorant of their partners’ need to receive a particular type of information; however, intelligence agencies do not generally disclose their “knowledge interests” for fear of revealing therein the targets of their operations (Lichtblau, 2005).

Randomness

Relying too heavily on a combination of powerful databases and automated tools to unmask potential terrorists increases the chances that there will be mistakes due to a randomness bias. Not only are records held by public and private databases notoriously unreliable but the emphasis placed on decontextualized relational features produces “false positives” and leads to the identification of innocents as terrorists. This lack of context partly stems from the fact that these tools are designed by engineers and computer programmers—instead of experienced investigators. For example, on the days following the events of September 11th, the owner of Seisint, an “information service” that sells data to private companies on potential customers, decided to use his expertise to create a program that could profile individuals who appeared to have certain characteristics that might suggest ties to terrorists (these people were allocated a “High Terrorism Quotient”). After weeks of code-writing and data extraction, his company provided to federal and local law enforcement agencies a list of 120,000 people who were deemed to represent a risk (O’Harrow, 2005: 102). One can only wonder how many names on that endless list of suspects provided genuine leads to overworked anti-terrorism investigators, and how many people with unconventional consumption patterns were flagged as potential jihadists. The determinist speculations at the core of datamining algorithms fail to account for life’s coincidences, which are not governed by the laws of causality.

Youssef Karroum, for example, was arrested at the US-Canada border on 27 January 2000 after traces of explosives were detected on the van he was driving. He was kept in detention for a week so that possible links with Ahmed Ressam (the man who tried to bomb Los Angeles International Airport during the millennium celebrations) could be investigated. Karroum was released once it became clear that the vehicle he was driving had been the property of a government agency that used it to transport fertilizer. (The nitrates used in the production of many industrial fertilizers are also an ingredient of choice for bomb-makers.) The precipitating factor in his arrest was the fact that his name had been “red flagged” by the FBI following Ressam’s arrest. Brandon Mayfield was also the victim of slipshod linkage analysis: an Oregon lawyer converted to Islam, his fingerprints were erroneously matched to print fragments found on the site of the Madrid 11 March bombings. It was, however, indirect associations with people suspected of terrorism (a publication in which he advertised his legal services, a charity called by his wife, and an Al Qaeda sympathizer he represented in a child custody case) that led to his arrest, despite early doubts over his guilt expressed by the Spanish authorities (O'Harrow, 2005: 174).

The "small world" principle and the few degrees of separation that connect us all mean that, theoretically, it is increasingly likely that we will be connected to an Al Qaeda terrorist through our friends and acquaintances (Barabási, 2002; Watts, 2003). This does not mean that we are more likely to participate in terrorist activities since, even if we were interested, the chances that we could reach this person easily are slim at best. Counterterrorism datamining software does not make such distinctions, and random connections can easily be misinterpreted when projected on aesthetically appealing relational charts that allegedly unveil hidden terrorist networks. SRD, a company recently acquired by IBM,[9] has developed a program called NORA (Non Obvious Relationship Awareness) that can identify social ties spanning 30 degrees of separation, more than enough to make everyone a potential suspect by association. This 21st century phrenology is grounded in a simplistic understanding of the properties of social networks.

Networks

As previously stressed, the concept of network is complex and comprises at least two different notions, that is, the notion of terms ("nodes") and their relationships ("links"). Both these components—terms and their relationships—must have a certain degree of determinacy to allow us to speak of networks. This does not seem to be the case at present in special interest policing in the US, where the identity and operation of the various nodes of the intelligence network are becoming increasingly blurred. The military are now involved in the collection of HUMINT, the CIA is increasingly operating within US territory, and the FBI is now recruiting spies to operate outside the country (Johnston & Fehl, 2005). The same trend is apparent in Canada, where the Canadian Security Intelligence Service, a domestic agency, is now beginning to operate abroad. When their identity becomes indeterminate, nodes tend to morph into networks, thus clouding the distinction between nodes and their links and making the use of the notion of network itself problematic. This caveat represents a clear invitation to apply the principle of parsimony in determining what constitutes a network, until a more thorough mapping of high policing networks can be performed.

The creation, conversion, and distribution of knowledge are not isolated acts but are embedded in social and institutional networks, whose function is to both include and exclude. Members of these networks use a particular social structure to collectively and informally produce knowledge. Once constituted, knowledge is hard to "detach" with consistency from the knower, in large part because it possesses a tacit and idiosyncratic dimension that resists organizational hierarchical intermediation processes (Brown & Duguid, 2000; Nonaka & Takeushi, 1995; Polanyi, 1967). As a result, a number of underground strategies relying on the strength of personal ties are used to tap into this reservoir of tacit knowledge. Sociological studies of police occupational cultures systematically highlight the power of narratives to convey meaning, exchange tips and provide guidance about the unpredictable nature of police work, in the areas of both patrol and investigations (Manning, 2003: 235; Shearing & Ericson, 1991; Waddington, 1999). Informal advice on difficult cases is also exchanged laterally between colleagues, with little regard for established procedures or thorough documentation to the upper echelons. The 9/11 Commission noted, for example, that, prior to the attacks, some FBI field agents and CIA analysts were initiating informal contacts with their counterparts in other offices and agencies to further investigate leads that had been discarded by their superiors (NCTAUS, 2004: 268–275).

High policing organizations, fully aware of this social dimension and pressured from all sides to end their compartmentalization, are attempting to harness the power of informal "knowledge networks" through the creation of integrated structures that act as connecting platforms. In the United States, the National Counterterrorism Center (formerly Terrorist Threat Integration Center) and the local Joint Terrorism Task Forces represent the most prominent efforts at integration. Canada has also moved to create Integrated National Security Enforcement Teams that bring together analysts from various law enforcement agencies. Didier Bigo and James Sheptycki have documented similar initiatives in Europe (Bigo, 1996; Sheptycki, 2002). But these hubs of information and knowledge can also function as tools of exclusion in political environments where control over intelligence is seen as a strategic asset.

A number of strategies are deployed within institutional networks by nodes that seek to maintain their dominance or unravel the status quo. For instance, a claim for centralization can be made in respect to certain areas of responsibility, forcing nodes to interact through a hub-and-spoke structure. The post-9/11 competition between the FBI and the CIA to coordinate domestic intelligence activities is an example of this trend (Priest, 2005). A second strategy is to form new clusters (or alliances) that shift the power balance within existing networks. The tendency of every major US agency with a role in counterterrorism to launch its own integrated team or centre is not the result of a sudden conversion to the benefits of information sharing. It is undoubtedly more indicative of the uncertainty currently governing the field and an attempt to position nodes in a way that will maintain relevance without losing control. Unfortunately, under the appearance of genuine intelligence sharing, this proliferation of initiatives will likely entail further fragmentation of existing knowledge. Finally, defensive strategies that limit the flow of data in order to protect its integrity—or comply with legal restrictions—must be mentioned. Knowledge in counterterrorism—as in every other area of human enterprise—is as much the product of social and political forces as of accurate information about possible threats.

Conclusions

The obvious conclusion of the previous findings and analyses is that there is a lot of theoretical work to be done before we can declare that we have entered a new era of policing—the third one in some 30 years—and are now thinking within a new paradigm, supported by the concepts of knowledge and of network. It would be a grave mistake, however, to assume that the attempt to articulate such a paradigm is misguided or that, however tentative it might be said to be, it ought to be rejected. Instead we should be more cautious and, more importantly, much more industrious. If, then, there is a great deal of work to elucidate and to articulate a paradigm of policing as knowledge work, why is it that this notion caught up very rapidly and that research seemed to believe in certain quarters that it had immediately struck gold?

To try to answer this question, we will tentatively invoke Habermas' (1972) notion of a "knowledge interest".[10] There is a perceptible knowledge interest—indeed, a knowledge profit—in characterizing the police as knowledge (information, intelligence) workers. The prototype of the knowledge worker is the (social) scientist who creates theories about policing. The characterization of the police as knowledge workers closes the gap between the theory of policing and the objects of the theory. The net gain is that there is no longer a fundamental heterogeneity between the police and the social scientist—as there is when the police are defined *à la Bittner* as a mechanism for the distribution of coercive force. The social scientist can actually substitute *reflexive knowledge* for field work, as the police can be seen as to some extent in the same business as academics.

Even granting—as we are willing to do, up to a point—that the police are increasingly involved with discourse, we suggest that distinctions should be made between various forms of discourse. The discussion should begin with broad and theoretically neutral notions, such as linguistic content or signifier. An attempt should then be made to try to distinguish between the various forms of semantic content: fiction, rumours, information, data, intelligence, knowledge and so forth. Not all that is said and believed is knowledge or even information. For instance, the numerous stories in the US *National Inquirer* about sightings of Elvis Presley after his death would not intuitively qualify as "information", as the word is used with respect to the media (hence the distinction between information and "infotainment"). The equivalent of these statements about Elvis—and about almost any kind of statement—can be found in the police files. Making such distinctions is crucial for the following reason. It may make sense to divorce knowledge from validity for forms of "knowledge" that do not generally entail harmful consequences if acted upon (everyday beliefs about what is "real" or news in the media[11]). This is not, however, the case with actionable information collected by the police or brought to its attention: police action is potentially harmful to individuals and may mean that they are deprived of their freedom. The requirement that police information or intelligence be *thoroughly validated* before being considered to be knowledge and acted upon is proportional to its potential for harm. This potential cannot be evaded and is in part enshrined in law. The insight that the police are to a significant extent knowledge workers is fruitful only to the extent that it does not rest on a theory of knowledge that divorces knowledge and validity as proposed by Berger and Luckmann (1966).

In a similar vein, the current trend in the use of the concept of network should be extended beyond the metaphorical to embrace the methodological advances made in the fields of sociology, ethnology, political science, and mathematics. This would allow us to start mapping the various nodes and links in the intelligence process. As we stated earlier, the complexity of this endeavour is fraught with challenges: depending on the level of analysis, the boundaries of nodes become fuzzy, links can be found inside nodes, and some of the latter can be analysed as networks in their own right.

Investigative journalists—supported by anonymous sources—are sometimes able to disclose dysfunctional episodes and provide factual background to our theoretical hypothesis. Despite the reluctance of high policing organizations to open a window for academy enquiry, the thorough investigation of open sources might lead researchers to emulate the press and provide an informative discussion of the workings of intelligence services. This gap in our knowledge constitutes an opportunity more than a curse, inviting us to focus as much on the features of knowledge work in policing and those who carry it out as on the complex structures that constrain or enable their daily routines. Classical policing studies, while busy determining what sets policing apart from other social functions, ascertaining the role of coercive force in police work, or charting the new privatized territories, have tended to underestimate the importance of the complex web of institutions that govern and deliver security. In the information society, where time and space are collapsing and uncertainty flourishing (Castells, 1996), knowledge work is irremediably embedded in these networked structures. To borrow a metaphor from the world of physics, what we need now is not a microscope, which allows us to observe the tiny details of "worlds within worlds", but a particle accelerator that can expose the forces and interactions that keep those worlds together.

Notes

[1] This point is justifiably stressed by Peter Gill (personal communication).

[2] In a recent interview with *Law Enforcement News*, Michael Scott, Director of the US Center for Problem-Oriented Policing declared that "the single biggest gap in the whole professionalization of the American police has been this absence of a body of knowledge [on problem solving]. It's the *big* missing ingredient" (Simonetti Rosen, 2004b: 9).

[3] In an interview with *Law Enforcement News*, the terrorism expert Brian M. Jenkins stated that "domestic intelligence gathering has been an area that local police departments have been very, very wary about" (Simonetti Rosen, 2004c: 10).

[4] For a more complete account, see Brodeur and Ouellet (2006 forthcoming).

[5] The identity of a police informant can be divulged only when necessary to protect an innocent suspect. This is the traditional common law doctrine formulated in the UK during the 18th century.

[6] See Québec (1980). One of us—Brodeur—was member of two bodies created to investigate the activities that surrounded the October Crisis of 1970.

[7] http://www.ic-arda.org/index.html

[8] See the *Security of Information Act* (R.S., 1985, c. O-5, s. 1; 2001, c. 41, s. 25), sections 8 and 13.

[9] www-306.ibm.com/software/data/db2eas.

[10] "Fundamental methodological decisions ... have the singular character of being neither arbitrary nor compelling. They prove appropriate or inappropriate. For their criterion is the metalogical necessity of interests that we can neither prescribe not represent, but with which we must instead come to *terms*. Therefore my first thesis is this: *The achievements of the transcendental subject have their basis in the natural history of the human species*" (Habermas, 1972: Appendix, 312, italics in text).

[11] We are aware that what is published in the media can have grievous consequences for one's reputation. Media mischief is limited by the possibility of being sued and by the low credibility enjoyed by the media.

References

Barabási, A.-L. (2002), *Linked*, Perseus, Cambridge.

Bayley, D. & Shearing, C. (2001), *The New Structure of Policing. Description, Conceptualization, and Research Agenda*, National Institute of Justice, Research Report, Washington DC.

Berger, P.L. & Luckmann, T. (1966), *The Social Construction of Reality. A Treatise in the Sociology of Knowledge*, Doubleday, Garden City, NY.

Bigo, D. (1996), *Polices en réseau: L'expérience européenne*, Presses de Science Po, Paris.

Bittner, E. (1990), *Aspects of Police Work*, Northeastern University Press, Boston.

Böhme, G. & Stehr, N. (eds) (1986), *The Knowledge Society: The Impact of Scientific Knowledge on Social Structures*, Reidel, Dordrecht.

Brodeur, J.-P. (1983), "High and low policing", *Social Problems*, Vol. 30, no. 5, pp. 507–520.

Brodeur, J.-P. (2005), Cops and spooks, in: Newburn, T. (ed.) *Policing. Key Readings*, Willan, Cullompton, UK.

Brodeur, J.-P. & Leman-Langlois, S. (2005, forthcoming), Higher policing or surveillance fiction, in: Ericson, R.V. & Haggerty, K. (eds) *The New Politics of Surveillqance and Visibility*, Toronto University Press, Toronto.

Brodeur, J.-P. & Ouellet, G. (2006, forthcoming), L'enquête policière, in: *Criminologie*, Les presses de l'Université de Montréal, Montréal.

Brown, J.S. & Duguid, P. (2000), *The Social Life of Information*, Harvard Business School Press, Boston.

Burt, R.S. (1992), *Structural Holes*, Harvard University Press, Cambridge MA.

Burt, R.S. (2004), "Structural holes and good ideas", *American Journal of Sociology*, Vol. 110, pp. 349–399.

Canada, House of Commons (1990), *In Flux but not in Crisis. Report of the Special Committee on the Review of the CSIS Act and the Security Offences Act*, Queen's Printer, Ottawa.

Castells, M. (1996), *The Rise of the Network Society*, Blackwell, Oxford.

Cayouette, S. & Brodeur, J.-P. (2004), "Le policier comme travailleur du savoir", *Revue Internationale de Criminologie et de Police Technique et Scientifique*, Vol. 47, no. 1, pp. 86–106.

De Lint, (2003), "Keeping Open Windows: Police as Access Brokers", *The British Journal of Criminology*, Vol. 43, no. 2, pp. 379–397.

Dupont, B. (2004), "Security in the age of networks", *Policing & Society*, Vol. 14, no. 1, pp. 76–91.

Ericson, R.V. (1993 [1981]), *Making Crime*, 2nd edn, Butterworths, Toronto.

Ericson, R.V., Baranek, P.L. & Chan, J.B.L. (1987), *Visualizing Deviance*, University of Toronto Press, Toronto.

Ericson, R.V. & Haggerty, K. (1997), *Policing the Risk Society*, University of Toronto Press, Toronto.

Ericson, R.V. & Shearing, C. (1986), The scientification of police work, in: Böhme, G. & Stehr, N. (eds) *The Knowledge Society: The Impact of Scientific Knowledge on Social Structures*, Reidel, Dordrecht.

Greenwood, P., Chaiken, M. & Petersilia, J. (1977), *The Criminal Investigation Process*, D.C. Heath, Lexington MA.

Habermas, J. (1972), *Knowledge and Human Interests*, Beacon Press, Boston.

Homer, R.C. (1919 [800BCE]), *The Odyssey*, W. Heinemann, London.

Innes, M., Fielding, N. & Cope, N. (2005), "The Appliance of Science?: The Theory and Practice of Crime Intelligence Analysis", *The British Journal of Criminology*, Vol. 45, no. 1, pp. 39–57.

Innes, M. (2003), *Investigating Murder. Detective Work and the Police Response to Criminal Homicide*, Oxford University Press, Oxford.

Innes et al. (2005),

Johnston. D. & Fehl, D. (2005), "F.B.I.'s recruiting of spies causes new rift with CIA", *The New York Times*, 11 February, p. A8.

Johnston, L. & Shearing, C. (2003), *Governing Security*, Routledge, London.

L'Heuillet, H. (2001), *Basse Politique, Haute Police: Une Approche Philosophique et Historique*, Fayard, Paris.

Lichtblau, E. (2005), "9/11 report cites many warnings about highjackings", *The New York Times*, 10 February, p. A1.

Lyman, P. & Varian, H.R. (2003). *How Much Information?*, School of Information Management and Systems—University of California at Berkeley. Available online at http://www.sims.berkeley.edu/how-much-info-2003 (accessed 23 December 2004).

Manning, P.K. (2003), *Policing Contingencies,* The University of Chicago Press, Chicago and London.

McCarthy, E.D. (1996), *Knowledge as Culture*, Routledge, London.

Morselli, C. (2001), "Structuring Mr. Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade", *Crime Law and Social Change*, Vol. 35, pp. 203–244.

Morselli, C. (2003), "Career opportunities and network-based privileges in the Cosa Nostra", *Crime, Law and Social Change*, Vol. 37, pp. 383–418.

National Commission on Terrorist Attacks Upon the United States (NCTAUS) (2004), *The 9/11 Commission Report,* W. W. Norton & Company, New York.

Nonaka, I. & Takeushi, H. (1995), *The Knowledge-creating Company: How Japanese Companies Create the Dynamics of Innovation*, Oxford University Press, New York.

Office of the Inspector General (2004), *The Federal Bureau of Investigation's Foreign Language Program—Translation of Counterterrorism and Counterintelligence Foreign Language Material*, Department of Justice, Washington DC.

O'Harrow, R. (2005), *Nowhere to Hide*, Free Press, New York.

Polanyi, M. (1967), *The Tacit Dimension*, Anchor Books, New York.

Priest, D. (2005), "FBI pushes to expand domain into CIA's intelligence gathering", *The Washington Post*, 6 February, p. A10.

Québec (1980), *Rapport sur les Événement d'octobre 1970* (rapport Duchaine), Gouvernement du Québec, ministère de la Justice, Québec.

Schmitt, E. (2005), "Pentagon sends own spy units into battlefield", *The New York Times*, 24 January, pp. A1, A9.

Searle, J.R. (1996), *Speech Acts. An Essay in the Philosophy of Language*, Cambridge University Press, London.

Shearing, C. & Ericson, R. (1991), "Culture as figurative action", *The British Journal of Sociology*, Vol. 42, no. 4, pp. 481–506.

Shelby & Senator, R.C. (2002), *Additional Views of Senator Richard C. Shelby, Vice-Chairman, Senate Select Committee on Intelligence*, US Senate, Washington DC.

Sheptycki, J. (2002), *In Search of Transnational Policing*, Ashgate, Avebury.

Sheptycki, J. (2004a), *Review of the Influence of Strategic Intelligence on Organised Crime Policy and Practice*, Special Interest Paper 14, Home Office, London.

Sheptycki, J. (2004b), "Organisational pathologies in police intelligence systems", *European Journal of Criminology*, Vol. 1, no. 3, pp. 307–332.

Simonetti Rosen, M. (2004a), "Terror-oriented policing's big shadow. 2004, a retrospective", *Law Enforcement News*, December 2004, pp. 1, 4.

Simonetti Rosen, M. (2004b), The *LEN* interview. Michael Scott, Director of the Center for Problem-Oriented Policing, *Law Enforcement News*, November 2004, 9–14.

Simonetti Rosen, M. (2004c), The *LEN* interview. Brian M. Jenkins, Rand Corporation terrorism expert, *Law Enforcement News*, September 2004, 9–14.

Singel, R. (2003), Immigrant Database Draws Fire, *Wired News*, 9 December, Available online at http://www.wired.com/news/privacy/0,1848,61519,00.html (accessed 29 December 2004).

United Nations Centre for International Crime Prevention (UNCICP). (2000), *Assessing Transnational Organized Crime: Results of a Pilot Study of 40 Selected Organized Criminal Groups in 16 Countries.* United Nations (the report was actually released in 2002).

US Congress (1997), *Report of the Commission on Protecting and Reducing Government Security* (Senator Daniel Patrick Moynihan, Chairman), US Government Printing Office, Washington DC.

Waddington, P.A.J. (1999), "Police (canteen) sub-culture: An appreciation", *The British Journal of Criminology*, Vol. 39, no. 2, pp. 287–309.

Watts, D. (2003), *Six Degrees: The Science of a Connected Age*, W. W. Norton & Company, New York.

Wellford, C. & Cronin, J. (1999), *An Analysis of Variables Affecting the Clearance of Homicides: a Multistate Study*, Justice Research and Statistics Association, Washington, DC.

Wittgenstein, L. (1953), *Philosophical Investigations*, The Macmillan Company, New York.

Cases Cited

Bisaillon v. Keable [1983] 2 S.C.R. 60

Solicitor General of Canada v. Royal Commission of Inquiry (Ontario Health Records) [1981] 2 S.C.R. 494