Policing & Society, Vol. 16, No. 1, March 2006, pp. 27–49

Routledge
Taylor & Francis Group

Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001

Peter Gill

Widespread concerns and controversies have erupted in the wake of 9/11 in relation to the structures and processes by which states acquire intelligence with respect to security threats. More specifically, the controversies have centred on the issue of "failure": first, to what extent did the 9/11 attacks reflect an intelligence failure on the part of US and other intelligence services and, second, how did most western intelligence services fail to identify the destruction or disposal of Iraq's weapons of mass destruction after 1991? Strenuous efforts have been underway since 2001 to develop more effective security governance both within and between nations. This article discusses these efforts to construct security intelligence networks with particular reference to developments in the US and UK, the main carriers of the so-called "global war on terror".

Keywords: Security; Intelligence; Networks; Terrorism; Oversight

Security: Surveillance, Governance and Intelligence

"Surveillance" is central to explaining modern governance including the behaviour of agents and development of structures. Though discussed in different ways by social theorists such as Dandeker (1990), Giddens (1985: 181–192) and Foucault (1991) there is a core of similarity in their definition of surveillance as constituted by two primary components: first, the gathering and storing of information[1] and, second, the supervision of people's behaviour. In other words, it is concerned with knowledge

Correspondence to: Peter Gill, School of Social Science, Liverpool John Moores University, Clarence Street, Liverpool L3 5UG, UK. E-mail: P.Gill@ljmu.ac.uk.

The initial version of this article was presented to the ESRC Seminar "Networks, Mobilities and Borders in the Global System", Oxford Brookes University, January 2005. My thanks to the other participants and the journal's referees for their helpful comments.

ISSN 1043-9463 (print)/ISSN 1477-2728 (online) © 2006 Taylor & Francis
DOI: 10.1080/10439460500399395

and power. In contemporary Western social theory, surveillance is seen both as the central aspect of the establishment of modern "sovereign" state forms (Giddens, 1985) and of the more recent decline of sovereignty as it is replaced by "governance" or, for Foucault, "governmentality" (1991) including the concomitant recognition of the significance of private forms of governance. Furthermore, studies of non-Western societies show that surveillance is similarly central there: its philosophical basis may be crucially different, for example, the rejection of individualism, but its core goals—understanding and control—pertain (Bozeman, 1992: 198–205). So, not surprisingly, global surveillance is argued to be an intrinsic part of the general economic restructuring of capitalism that is referred to as globalisation and post-9/11 developments have served only to accelerate this already existing trend (der Derian, 1992: 46; Lyon, 2003; Whitaker, 1999 provides an excellent survey of these developments). The security intelligence[2] processes with which we are specifically concerned are essentially a sub-set of the more general surveillance that constitutes contemporary governance. Thus, since intelligence is one of the two defining components of surveillance and, in turn governance, then security intelligence is one of the defining components of security governance.

Clearly we must incorporate an analysis of corporate and other non-state security agents as part of the general shift towards "security governance". Noting the current "pluralisation" of security governance, partly through privatisation but also because of the role for private concerns enabled by property law, Johnston and Shearing argue for the adoption of a nodal (network-based) rather than state-centred conception of governance. They identify four sets of governmental nodes: state, corporate, non-governmental organisations (NGOs) and the informal or voluntary sector (Johnston & Shearing, 2003: 144–148). Yet, although security *intelligence* is central to security *governance*, Johnston and Shearing say very little explicitly about the role of intelligence. This needs to be corrected lest it remain the "missing dimension" of historical and government studies (Andrew & Dilks, 1984; Hoare, 2002).

Security Networks

At root, the idea of networks is "of informal relationships between essentially equal social agents and agencies" (Frances et al., 1991: 16). Both informality and "essential equality" are, indeed, significant in security networks: informality because this is how they have developed in the first place—as links made between security agents for the sharing of information—and "essential equality" because, in contrast to the ranks of formal super- and sub-ordination in police departments, what matters in the network is that you are trusted and have information with which to trade. However, neither of these tells the whole story: on the one hand we see the slow but steady development of *formal* networks between security agencies *via* treaties and formal legal agreements and, on the other, some agencies and some agents are clearly more equal than others in their ability to structure networks and operate within them. Security does not depart from the general rule that networks:

> link up different places and assign to each one of them a role and a weight in the hierarchy of wealth generation, information processing and power making that ultimately conditions the fate of each locale. (Castells, 2000: 445)

One reason why networks are potentially most useful for the study of developments in policing and security is that they provide an umbrella concept for comparative study. In what has become a commonly-deployed device, it has been suggested that markets, hierarchies and networks represent the three dominant modes in which social life is co-ordinated (Thompson et al., 1991). Applying this idea to policing we can see how *markets* is the organisational logic for corporate providers of private security and *hierarchies* for traditional state policing but what is the underlying model for the provision of security by NGOs and voluntary groups of citizens? The answer can be found in what Leishman (1999: 121–122) describes as the *communitarian* orientation in policing that has been most pervasive in Asia although aspects have been "borrowed" by police elsewhere? To be sure, this is a very wide category that can incorporate neighbourhood watch schemes, victim support, Guardian Angels and, at the extreme, vigilantism. No particular position is taken here as between the variants of communitarianism (Hughes, 2000); the term is used simply to describe security provision that is neither commercial nor statist and thus in effect combines the third and fourth nodes identified by Johnston and Shearing above.

But where do *networks* fit in, then? Although *individual* security providers are likely to be located quite clearly within a market, state or community model, we may well find *elements* of two or all three different models within any single provider, for example, a public police force whose dominant strategy is "community policing" and which charges citizens for services such as policing sporting events. The strength of networks is that they can map the multifarious connections *between* policing agencies whatever the precise mix of market, hierarchy and community they embody. Further, it can be suggested that networks are the most general category of coordination: the market resembles a security network of firms in price competition and their customers; hierarchy is a network of bureaucratically-organised public police departments and community is constituted by a network of voluntary and non-governmental residents and victims groups (cf. Frances et al., 1991: 16–18). The actual mix of these forms sets up tensions: for example, informal intelligence-sharing between police officers may develop out of frustration with the rule-bound and time-consuming formal procedures required within bureaucracies (e.g., Sheptycki, 2004: 23–24). This has significant implications for oversight, to which we return at the end.

Mapping Intelligence Networks

> Network analysis, by emphasizing relations that connect the social positions within a system, offers a powerful brush for painting a systematic picture of global social structures and their components. The organization of social relations thus becomes

> a central concept in analysing the structural properties of the networks within which individual actors are embedded, and for detecting emergent social phenomena that have no existence at the level of the individual actor. (Knoke & Kuklinski, 1991: 173)

Figure 1 is an attempt to paint a picture or map of the "territory" within which police and security intelligence networks develop. This territory is as much symbolic as physical now—while much greater use is made of information and intelligence in order to support traditional policing of people and spaces, so there have been major developments in the policing of information flows themselves (Manning, 2000). Drawing a map is the relatively easy part of deploying network analysis—what is much harder is moving beyond metaphor to analyse the extent to which the network structure is an independent variable distinct from merely the actions of individual actors (cf. Dowding, 1995; and see Brodeur & Dupont, this issue). Ironically, perhaps, our endeavours to understand security networks mirror those facing intelligence analysts when they map criminal or terrorist networks. For all of us, providing structural maps is a complex but essential pre-requisite to attempt to explain how networks operate and why.

Globalisation—the process that has brought about the current territory for policing and security—manifests itself along three dimensions: a "deepening" of levels so that there is increased interaction between local and transnational developments; a "broadening" of sectors that are involved in governance; and, third, spatial "stretching" so that developments in one part of the globe can have immediate and world-wide impact (McGrew, 1992). All three account for contemporary policing networks but it is the first two that are discussed below since they have the most significant impact on organisation and doctrine.

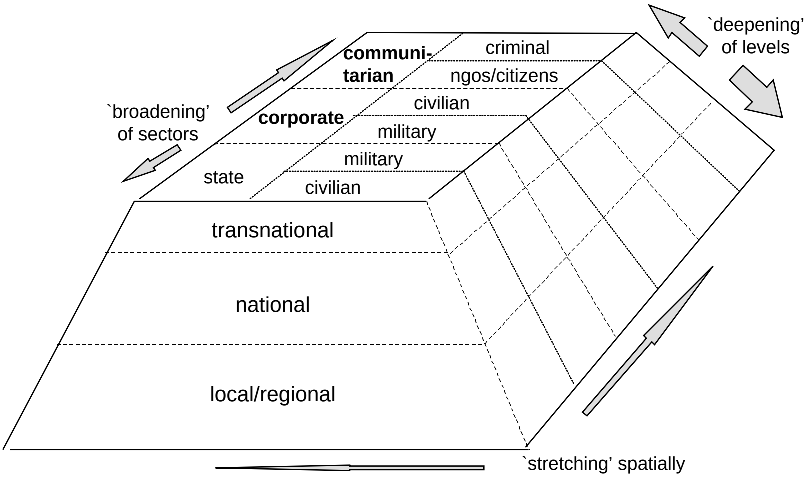

Figure 1 Global Security Networks

Levels

It is common in social science to analyse phenomena at different levels, not because they are sources of explanation in themselves, but because they are useful objects for analysis defined by a range of spatial scales (Buzan et al., 1998: 5). Similarly, we are used to the idea of theory operating at levels such as macro-, meso- and micro-. In the modern era policing has been organised by states but actually located organisationally at different levels. For example, in the UK it was organised in the 19th century at *local* level in (urban) boroughs and (rural) counties and the US developed similarly in municipalities and counties. Since then, there has been a steady reduction in the number of UK forces so that they tend towards the *regional* but in the US there has been no equivalent move to amalgamations. Policing in France always was essentially *national*—both national forces are organised within central government departments. *Transnational* policing is essentially of two types: mainly it consists of cross-border contacts between national or local police forces; but there are now examples of policing by supranational bodies (Johnston, 2000b: 21).

Sectors

The three main sectors identified in Figure 1 coincide with the policing models discussed above: the state (organised in bureaucratic hierarchies), corporate security (competing in markets) and non-governmental organisations and voluntary associations (communitarian). There are, of course, many sub-divisions within each of these sectors. The most obvious division within the state sector is between civilian and military agencies, the former usually divided into "police" and "security" and the latter into the separate services. Police intelligence developed only slowly in the UK: a Special Branch was first formed in the Metropolitan Police in 1883 but it was the 1960s before all forces formed their own. Specific criminal intelligence squads were, again, established first in London after the Second World War and by the mid-1970s all forces and their constituent divisions had some criminal intelligence capacity, though it was often poorly-developed. Regional criminal intelligence offices were created in 1978 to complement the work of the regional crime squads and in the 1990s the National Criminal Intelligence Service (NCIS) was formed from the merger of the regional offices but also incorporated Customs personnel and civilian analysts. Also in the early 1990s, arguably in the face of the discrediting of then current crime control policies, the notion of "intelligence-led policing" was promulgated with the intention of intelligence techniques being applied not just to organised but also to volume crime. To reinforce this, a National Intelligence Model was published in 2000 (Flood, 2004; Gill, 2000: 77–91; Grieve, 2004; see Gill, 2000: 98–128 for equivalent discussion of developments in Canada and USA).

"Security intelligence", normally organised at the national level, was established bureaucratically about 100 years ago in both UK and US. In the UK both the domestic security intelligence agency (Security Service or MI5) and Secret

Intelligence Service (SIS or MI6, covering foreign intelligence) were set up in 1909 and the US Federal Bureau of Investigation (FBI) dates from 1908. As a police agency, the FBI has always struggled to face in several different directions. Hoover's development of domestic political intelligence programmes from the 1930s onwards led to massive scandal after his death and the Bureau re-oriented towards white collar and organised crime in the 1970s though it retained responsibility for counter-intelligence (e.g., Poveda, 1990). In the wake of 9/11 strenuous efforts have been made to refocus the Bureau away from "law enforcement" and back towards security intelligence, an issue we shall discuss further below. The FBI is formally located within the Justice Department that contains also the Drug Enforcement Administration—another agency much involved in intelligence. The other five national civilian intelligence agencies are located in the Energy Department (covering, for example, nuclear proliferation), the Bureau of Intelligence and Research in the State Department that draws on diplomatic reporting, the Treasury Department (covering *inter alia* taxation and money laundering) and the Central Intelligence Agency (primarily for foreign intelligence and equivalent to MI6). The newest kid on the US domestic intelligence block is the Information Analysis and Infrastructure Protection (IAIP) division of the Department of Homeland Security established in the wake of 9/11. It is not intended that IAIP conduct its own intelligence operations but that it should conduct assessments of the information from its own personnel such as border guards and secret service plus whatever is shared by CIA and FBI (Jordan, 2005).

In the UK and US state military intelligence is basically organised within each service plus some mechanism for joint assessments; in the UK, for example, the Defence Intelligence Staff (DIS) provides a central assessment process for military. In the US the parameters of organisation are similar but complicated by the sheer size and extreme fragmentation of the military and intelligence establishment. In the US there are nine national intelligence organisations within the Defense Department: one for each of the four Services; the Defense Intelligence Agency that both runs military espionage agents and provides assessments similar to the DIS in UK; the National Reconnaissance Office (NRO) with responsibility for spy satellites; and the National Imagery and Mapping Agency (NIMA) that interprets satellite photography and prepares world maps. Finally, the National Security Agency (NSA) collects signals intelligence (SIGINT) and provides code-breaking (Johnson, 2002: 2–3). Both the NSA and its UK equivalent—Government Communications Headquarters (GCHQ)—straddle the civil-military divide (Smith, 2003 provides a readable survey of all the UK agencies).

In the corporate sector there are a whole range of security providers. These are divided into civilian (or security) and military in Figure 1 since some companies are fairly clearly one or the other but others operate within both sectors. Distinguishing between private security (PSCs) and private military companies (PMCs) is useful since they are likely, respectively, to be deployed defensively or offensively but in practice, especially in conflict zones, they are likely to merge (Schreier & Caparini, 2005: 1). There is now extensive literature on private security in general, for example, Shearing and Stenning (1987), Johnston (1992, 2000a) and Button (2002) but less on the extent to which "intelligence" is a specific part of these activities (Hulnick, 1999: 151–171 provides a general survey of "spying for profit" in the US; see also Block, 1992; Marx, 1988).

Corporate security tends to be organised either in specialist departments or provided by outside contractors. The security sector has seen a wave of mergers and acquisitions in recent years, for example, in July 2004 Securicor and Group 4 merged into a group whose joint turnover in 2002–03 had been £3.8 billion. Both groups are best known for their provision of technical security systems and guarding and patrolling services but they still offer "consultancy and risk audit services" that incorporate elements of security intelligence (www.group4securicor.com). The group's US-based division is Wackenhut, whose Consulting and Investigation Services offer forensic accounting, fraud detection, litigation support (including case and document analysis), investigative due diligence (when dealing with new customers and potential partners), surveillance (for example, videotaping suspected incidents) and undercover services where "A skilled investigator, posing as an employee, is placed into an unsuspecting workforce to gather information on workplace problems." Acknowledging the problems of providing a wide diversity of expertise around the globe, Wackenhut has sought to develop its own network of "Strategic Alliance Partners" (www.ci-wackenhut.com). Securitas, founded in Sweden in 1934 embarked on an aggressive acquisition policy in the 1990s taking over well-known firms such as Burns International and Pinkerton. The acquisition in 1999 of Pinkerton, with its greater emphasis on investigative services, made Securitas the world's largest security company. Offering a range of security systems, security services and cash handling the company strategy is continued expansion from its current position of having 8 per cent of the global security market (Johnston, 2000b: 28–29; www.securitas.com). Pinkerton, in turn, has outsourced its Global Intelligence Services to iJET Travel Intelligence Link who provide clients with travel-related intelligence relating to security, financial, legal and other factors for more than 460 destinations. Clients may also obtain daily intelligence briefings, monthly intelligence reviews, country security assessment services and other "travel risk management solutions" (www.pinkertonagency.com/global/services.html).

Control Risks Group, founded in 1975, appears to bridge the civilian and military sectors, offering to government and corporate clients a range of services including political and security risk analysis, investigations, pre-employment screening, crisis management and information security. Political risk analysis includes due diligence investigations into potential partners, especially in countries where risks and uncertainties exist, including "where single-issue action groups are active". Thus these risks extend beyond the normal concerns with violence or kidnap into criminal and environmental areas and are examined through a Total Risk Assessment Methodology (TRAM) that identifies, evaluates, assesses and offers management advice on the handling of risk (www.crg.com/html/service_level3.php?id = 362). The current occupation of Iraq has seen the involvement of unprecedented numbers of private military personnel and contractors (Singer, 2004) and Control Risks has established a project office there that is, so they claim, providing security management services for government departments, companies and NGOs (www.crg.com/html/service_level3.php?id = 588). Military Professional Resources Inc (MPRI) was founded in 1987 by eight retired military officers and is engaged primarily in military contracting but with law enforcement expertise also. It is not large in terms of the number of employees (1,500) but draws its workforce on a contracting basis from a database of more than 12,500 former military and other personnel. It was involved in South East Europe in training both the Bosnian and the Croatian armies and is generally credited with carrying out, at one remove, the US policy of neutralising the Serb military in the mid-1990s (Johnston, 2000b: 34; Singer, 2003: 124–130; www.mpri.com/site/about.html).

Non-governmental organisations may also be included since they have a crucial presence in areas of insecurity and carry out their work in conjunction with state agencies. Personnel involved in aid, migration or peacekeeping functions may well find themselves, knowingly or unknowingly, part of security intelligence networks. Deibert (2003) identifies the parallel development of citizen intelligence networks from the emerging of NGOs, activists and computer hackers. Individuals and voluntary groups are involved in local security networks in various ways, for example, "gated" communities—either horizontal on private estates or vertical in apartment blocks—or other neighbourhoods may buy in the services of a private contractor and neighbourhood watch schemes seek to mobilise collective community resources. Communities based on shared cultural beliefs and practices may also provide the basis for organising security and individuals have always provided for their own security *via* the right of self defence, though some have always been able to afford a great deal more than others (Bayley & Shearing, 2001: 7–9).

The issue of citizens deploying self-defence can be quite controversial—witness the recent debate in the UK as to just how much violence householders should be permitted to use on intruders but there is less ambiguity when it comes to individuals involving themselves in information gathering. For example, *Crimestoppers* is an innovation by which individuals who provide confidentially information leading to an arrest or conviction may be paid a reward, funded by the private sector (Gill, 2000: 188–189). After 9/11 US Attorney General John Ashcroft sought to introduce a programme called TIPS whereby millions of American workers would involve themselves in reporting suspicious behaviours or people but the scheme foundered on a wave of opposition. Yet some still envisage a much wider role for citizens than merely that of self-defence. Robert Steele argues vigorously for a "citizen-centred intelligence" on the grounds that the public—the "intelligence minutemen of the twenty first century"—can only rely on themselves, not elites, to protect their interests (Steele, 2002: esp. xiii–xviii).

Finally, we need to acknowledge the place of illegal organisations. First, they are themselves most likely to resemble networks: the idea of criminal networks provides a common discourse among investigators and analysts and they use social network analysis (SNA) in order to map the networks specifically to identify their strengths and weaknesses in order to formulate strategies of attack (Klerks, 2003; Sparrow, 1991). But, crucially, they may, on occasions, be involved in networks with formally legal ones, for example, if state agencies wish to "sub-contract" illegal operations because of the risks they run if exposed. This may involve just information-gathering but, far more controversially, state agencies might sub-contract *covert action*, for example, the use by CIA of organised crime to attempt to assassinate Castro in the 1960s (Johnson, 2002: 182–182), the deployment of "death squads" by authoritarian regimes in several Latin American countries and the "collusion" between British intelligence and loyalist paramilitaries in the assassination of Republicans in Northern Ireland (see further below). There is a wide variety of groups that might be involved: some might amount to "para-states" that challenge the state's legitimate monopoly on the use of force, others will be criminal enterprises and yet others will be national liberation movements. At different times any of these may be agents of state intelligence and therefore be part of a broader network of security governance (Bayley & Shearing, 2001: 6–7; www.fas.org/irp/world/para/scope.htm).

Networks might develop within and/or between any of these three dimensions. States or corporations will often appear to be the "dominant node" or partner in a security network but Johnston (2000b: 38) suggests that, in general, the most productive view to take is of:

> a changing morphology of governance in which partly fragmented states interact with commercial, civil and voluntary bodies both within and across national jurisdictional boundaries.

Similarly, Deibert identifies "transnational networks of citizen activists weaving in and around the traditional structures of state interaction" (2003: 189). Security companies and NGOs themselves maintain intelligence capacities in network form as they operate globally and within specific nations and localities, that is, as a form of multi-level governance. The development of "local security networks" between agencies both public and private (e.g., Gimenez-Salinas, 2004; Jones & Newburn, 1998) and citizen groups (Johnston, 2000a: 167–175) provides a clear example of cross-sectoral networks and other examples can be found at regional, national and transnational levels. Iraq in early 2005 may provide only the most dramatic instance of a global trend. Clearly there must be some shared interest in order to bring the actors into the network in the first place but the actual nature of relationships must be subject to empirical validation and conflicts may occur between nodes within networks. These will arise for a variety of reasons, within the state sector, for example, agencies have different mandates and objectives that sometimes overlap but sometimes do not; corporations may agree some joint project but they are also in a competitive relationship. Conflicts will be resolved depending on the relative power of the actors; in some cases they may lead to some restructuring of the network. In all of this we must not forget the impact on security networks of those who are their objects. We have already seen that groups who are the primary targets of security may, under certain conditions, become part of the network. Also, the way in which the targets react to attempts at information gathering and repressive action may have an impact on the form of the network as it has to adjust further—thus networks become protean (cf. Dorn, 2003.)

But the reality of intra-network conflict is not the only reason they are far from "seamless"—to the great frustration of authorities and practitioners. The organisational boundaries between intelligence agencies (represented in Figure 1 as dotted or broken lines between sectors and levels) interrupt the flow of information; although borders may be transformed or blurred they will remain, even if redefined. Also, the traditional "border-maintenance" conducted by hierarchies ensures the ubiquity of "bureaucratic politics" and will remain a structural barrier to network flexibility. But as well as being blocked at the borders, information may just locate in voids where no agency has an immediate interest or adequate resources to analyse or otherwise deal with it (cf. Gill, 2000: 54–57, 246–249). The sheer quantity of security data within information systems far outstretches their capacity to analyse it (Brodeur & Dupont, this issue). Therefore a more accurate image of Figure 1 would be to present it as an "exploded" diagram that incorporates both the borders between agencies operating in whatever sector, level or space and the voids into which information "disappears" (Figure 2).

Crossing the Borders and Bridging the Voids

There are many issues raised by the rapid development of security networks, both formal and informal; the rest of the article concentrates on questions of network management and oversight.

Network Management

Kickert and Koppenjaan (1997) suggest that network management has two main features: "game management" and "network structuring". The former includes:

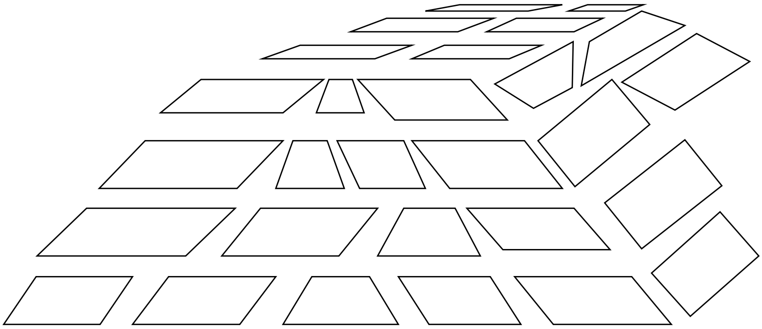

Figure 2 A Geology of Security Networks

activating networks in order to address a particular problem and arranging for the interaction of those actors who can help (activation); bringing together otherwise disparate actors, problems and solutions (brokerage); creating the conditions for favourable developments (facilitation); and, when conflict arises, providing mediation or arbitration.

We can identify a number of recent developments in security intelligence that illustrate these activities—all of them present to some degree before 9/11 but accelerated thereafter. A combination of factors have led to the activation of increased public-private networks. After the end of the Cold War the size of state intelligence agencies was reduced while their corporate cousins were increasing the scale and range of their activities. Therefore, although the budgets and personnel of the state agencies have been significantly increased since 9/11, the fresh perception of a range of asymmetrical threats across a wide variety of locations has brought into play increased public-private co-operation.

Barriers to information sharing and operational co-operation are an inevitable by-product of specialisation within state hierarchies and are aggravated in intelligence work by the high premium placed on source protection and general reluctance to pool "sensitive" information (Aldrich, 2004: 732; Brodeur & Dupont, this issue). The main form of "brokerage" to be found in the intelligence community—before and since 9/11—has been "fusion centres" or "task forces". Representatives from several agencies are brought together, each with access to their home database, so that they can combine the analytical resources of otherwise separate agencies on a targeted problem or person by overcoming the incompatibility of different databases or privacy restrictions on the sharing of information. Examples include the US National Counterterrorism Center that incorporates the CIA's Counterterrorism Center (CTC) and FBI Counter Terrorism Division and, in the UK, the Joint Terrorism Analysis Centre (JTAC) with personnel from MI5, SIS, GCHQ, DIS, police SB and the Security Division of Transport Department (Intelligence and Security Committee, 2003: 18). In terms of the map, these centres act as "bridges" across voids and may provide partial solutions (cf. "police archipelagos", Bigo, 2000). Over time, however, task forces may also become part of the problem to the extent that they become institutionalised and cease to "facilitate".

The main attempt at facilitation has been to break down borders. One manifestation of this has been increased interdisciplinarity. Until the later stages of the Cold War, the various intelligence "disciplines" remained clearly demarcated. Within the state sector, foreign, military and criminal intelligence were largely separate and the last struggled to achieve legitimacy within its own field of law enforcement, let alone in the broader world of intelligence. Steadily, a number of factors have reduced the disciplinary barriers, for example, the occurrence of terrorism from late 1960s onwards (a phenomenon with foreign, domestic, political and criminal relevance) brought security and police agencies into closer contact (though the process is seldom smooth). The end of the Cold War hastened these developments, for example, in 1992 the UK Security Service took over from

Metropolitan Police responsibility for intelligence regarding Irish Republican terrorism in Britain and then acquired a role in gathering intelligence regarding serious crime (Brodeur, 2005 discusses the implications of increased co-operation between police and "spooks").

Other post-9/11 attempts at facilitating networks have addressed technological and political issues regarding access to and combining information—in both public and private sectors. Not only have extra powers for technical collection been sought but also, throughout the US and Europe, agencies are seeking improved access to electronic data collected by others. However, access to specific databases is one thing, bringing together multiple databases is another. The "big idea" since 9/11 is the "mining" of "data warehouses" constructed by linking public and private databases. This has been made technically possible by XML (Extended Markup Language) software that enables previously separate databases to be "merged" *via* a universal language and mining "involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets" (Seifert, 2004: 1).

Some of the examples being considered in the security field are truly awesome: inspired by the conclusion that in the period before 9/11 there was a failure within the intelligence and law enforcement communities to "join the dots" between items of information already in the system, major efforts are underway to seek solutions. For example, in a report commended by the 9/11 Commission, the Markle Foundation proposes a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network that will enable information sharing by federal, state, local government and private sector users. It provides, *inter alia*, an overview of the "landscape of available data" including 26 "data sources" (such as communications, corporations, courts, insurance, licensing, marketing, medical, memberships, real property, travel) and 150 types of record (benefits, car rentals, voter registration, prescriptions, video rental loan applications, visas . . .), current availability (free or for purchase) and sets out what it believes the President, Congress and specific departments should be doing to create the appropriate architecture (Markle, 2003). In summary, it is impossible to do justice to the breadth of vision within the report bordering as it does on the utopian—or, perhaps, dystopian. Progress is being made on the technical issues but what can be said without doubt is that it reflects an enormous faith in the possibility of a technological fix to a highly complex problem—human security—and that nothing in the history of the extraordinarily fragmented American intelligence and law enforcement communities suggests that it has the slightest chance of being achieved.

Ideas in the UK are somewhat more prosaic. The Security Service and police special branches already have networked communications but initial plans for a general national police intelligence system were dropped from the National Strategy for Police Information Systems (NSPIS) in 2000. The Police National Computer provides for a mechanism by which forces can check on previous *convictions* but there is no equivalent system for *intelligence*. It is planned to have one in place by the end of

2005. New plans have been triggered, not by 9/11, but by the Bichard inquiry (2004) into the case of Ian Huntley, convicted in December 2003 of the murders of two young girls in Cambridgeshire, that revealed the chronic state of information management in two English police forces and the wide gulf between the rhetoric of "intelligence-led policing" and the reality (Gill, 2004/05). It is intended that a national system for police intelligence sharing (IMPACT) will be in place during 2007 (Home Office, 2005a). Given the recent dismal record of large government ICT projects in the UK we shall be best not to hold our breath. Meanwhile the Home Office has announced that the intelligence services, but not the police, will have access to the central register that will provide the basis for the government's ID cards scheme (Morris, 2004). Since the Government claims that ID cards are targeted at fraud and terrorism, we should not be confident that the exclusion of police will last long.

Mediation or arbitration might be provided in networks by some of the innovations already discussed such as task forces or individuals who routinely "cross" agency boundaries. An excellent example of this is the liaison officers studied by Bigo whose *raison d'être* is mediating between, if not transcending, different sovereignties:

> networks of control agents who see as their primary task the maintenance of public order, broadly conceived, and who distance themselves from all political reasoning. All over Europe there are thousands of control agents working together every day; in so doing they are breaking down the myth of national sovereignty. (Bigo, 2000: 85)

But perhaps the person who has now taken on the largest mediation job of all is John Negroponte, formerly US Ambassador to the UN and lately Iraq who, as the first Director of National Intelligence in the US, has budgetary authority over the 15 federal intelligence agencies. Only time will tell whether he will actually convert his formal authority into real impact on a network dominated financially by the Pentagon (Johnson, 2002: 109–111).

A number of factors condition the ability to manage networks. For example, first, diversity—the higher this is the more likely that management will only be possible at a distance (and the diversity of the US intelligence network is extremely high). Second, intelligence networks are "closed" or self-referential systems. Because of secrecy the networks are harder to manage except to the extent that their self-regulatory capacity can be utilised. Self-regulation is a characteristic of "professions" and, as recent controversies around intelligence assessments of Iraqi WMD in the lead-up to the 2003 invasion show, professionalism among analysts is much needed as an essential (but not necessarily successful) counterweight to "politicisation". But such "self-regulation" can also operate negatively, for example, it might sustain "groupthink".

Third, how extensive are the conflicts or convergence of interest? Beyond the simplistic rhetoric of "all being on the same side", different agencies have varied legal mandates and, given their extensive discretion to identify priorities, may well have even more varied short- to medium-term organisational goals.

Fourth, what is the political and social context within which the network operates and is there the political will and skill to manage in the desired direction? A high profile for the "problem" in politics and the media will increase the pressure on organisations to commit the resources required for collaboration and, where different legal frameworks are in existence, action might be taken by the agency operating within the most permissive legal context.

Fifth, management is facilitated if previous contacts have produced a desire to reciprocate. People do not like passing on information obtained possibly at high cost if they worry about the unpredictable consequences of losing control over it or they may just fear someone else getting the credit for an operation. Security concerns may be real or exaggerated but they will increase the more extensive the network over which the information will be dispersed.

Sixth, given broad mandates and limited budgets, the costs of an operation (whether aimed at "intelligence" or an investigation) will be a prime consideration. The more specific and credible information is, the more likely it is to lead to commitment of additional resources. The greater the complexity of a case in terms of jurisdictions and agencies involved, the more likely it is that a formal agreement will need to be negotiated between the contributing agencies, identifying who will do what.

"Network Structuring"

This becomes an issue to the extent that problems cannot be "managed" within existing organisational frameworks. The "misfit" between the structure of the US intelligence network and the task of preventing terrorist attack was clear to many well before 9/11 (e.g., Travers, 1997). Now, some institutional restructuring has become a political imperative for the Administration and the Department of Homeland Security is the main result. It is hard to see how this will succeed beyond the level of symbolic politics, for example, the constituent agencies will keep their varying mandates that will prevent them from becoming simply the counter-terrorist intelligence clearinghouse that some desire. The enterprise appears driven by a belief in the possibilities for hierarchical co-ordination rather than the creative possibilities of networks.

But even this restructuring affects only the national level; by comparison the regional and local law enforcement community is positively atomistic. Quite how are the approximately 18,000 law enforcement agencies at federal, state, local and tribal levels to get their act together?

> Every law enforcement agency in the United States, regardless of agency size, must have the capacity to understand the implications of information collection, analysis and intelligence sharing. Each agency must have an organized mechanism to receive and manage intelligence as well as a mechanism to report and share critical

> information with other law enforcement agencies. In addition, it is essential that law enforcement agencies develop lines of communication and information-sharing protocols with the private sector, particularly those related to the critical infrastructure, as well as with those private entities that are potential targets of terrorists and criminal enterprises. (Carter, 2004)

The task is immense: bearing in mind that a significant number of these agencies are one- or two-person strong, it defies comprehension.

There have been fewer demands for restructuring in the already unitary governmental structure of the UK but one relevant innovation is the creation of a Serious Organised Crime Agency (SOCA). This is less a reaction to 9/11, however, than unfinished business as it, in effect, merges NCIS and the National Crime Squad. Sir Stephen Lander, Director General of the Security Service 1996–2002, will chair SOCA (Home Office, 2004). As of February 2005 the Bill states the function of SOCA to be:

> gathering, storing, analysing and disseminating information relevant to—
> a) the prevention, detection, investigation or prosecution of offences, or
> b) the reduction of crime in other ways or the mitigation of its consequences. (Home Office, 2004: s.3[1])

Thus the Agency is clearly in the intelligence business.

Network structuring takes place also transnationally: in Europe, for example, the Berne Group was formed in 1971 by 6 European internal security agencies and now includes 17, the most recent joiner being Greece. Following 9/11 the Berne Group created a new organisation called the Counterterrorist Group (CTG) with a wider membership of EU intelligence and security services plus the US, Switzerland and Norway. CTG is mainly concerned with threat assessments regarding Islamic terrorism and since the Madrid bombings has been playing a major role in implementing intelligence-related aspects of the European Council's Declaration on Combating Terrorism. In 1994 the Middle Europe Conference was set up at the suggestion of the Dutch and assisted the preparation for accession of the ten new countries in 2004 (Aldrich, 2004: 738–739).

Oversight of Networks?

Events since 9/11 have reversed the swing of the pendulum of democratic control and oversight of intelligence. Scandals produce a reaction in which the main concern is to establish political control of the agencies and/or their oversight by external parliamentary or judicial committees. Intelligence "failures", on the other hand, have the opposite effect as concern shifts away from agencies' propriety towards their effectiveness. Arguably this is a serious error since there is no evidence that sacrificing propriety "in the interests" of security has the desired effect, other than in immediate operational circumstances, and even there, the so-called gains may be illusory. Rather, legality and democracy should be seen as essential components of security (e.g., Lustgarten & Leigh, 1994: 3–35).

The Weakening of Due Process

Since 9/11 we have witnessed a classic example of "securitisation" in which the terrorist threat has been presented as existential, thus requiring emergency measures outside the normal bounds of procedure (Buzan et al., 1998: 23–26). Traditionally, the main distinction made between intelligence and law enforcement was that police were interested in bringing people to court and therefore had to develop *evidence* rather than just *intelligence*—evidence requiring a higher degree of certainty as "knowledge". As UK police started to embrace "intelligence-led policing" from the early 1990s onwards, they adopted techniques such as targeting and surveillance (both technical and human) in an effort to increase their effectiveness and meet increased performance measures imposed by government. Although "crime prevention" had always been a formal objective of police, it received fresh impetus as police adopted "disruption" as a tactic, specifically, seeking to take actions that prevented the commission of a crime or disrupted the operations of a crime market such as a supply chain without necessarily seeking to prosecute the perpetrators. There was a steady increase in arrests through the 1980s and 90s but no concomitant increase in formal cautioning or prosecution (Hillyard & Gordon, 1999). The advantages of informal approaches for police are clear: they are quicker and cheaper because they rest on a lower evidential burden than prosecution but they raise the potential for corruption and involve a lack of transparency that endangers rights (Gill, 2000: 252–256). Similarly, as noted by Bayley and Shearing, private security can exclude people on the basis of presumptive signs of deviancy, public police can exclude only by incarceration (or "tagging") on the basis of conviction (2001, 18). The spread of anti-social behaviour orders (ASBOS) in the UK and more general shift towards "risk-based" policing (Johnston, 2000a) modifies this slightly but the point remains. The same issue arises in the military field: Johnston (2000b: 35) quotes a US official:

> I have a problem with the privatization of US foreign policy and national security policy. . . . It gives you what the intelligence community have had for a very long period of time: plausible deniability. It is a way of getting things done that the administration doesn't have to go to the Hill or to the American public to talk about.

These dangers have been increased not just by the adoption of intelligence techniques by police but by the changed legal conditions under which security intelligence agencies themselves operate. Hitherto, the concept of the "rule of law" has been taken to mean, broadly, that officials acting in the name of the state are subject to the same legal restrictions on their behaviour as any other citizen and that, should they transgress the law, they will be held accountable. Although this states an ideal rather than a working description of government, it remains a significant way by which we discriminate between regimes that we identify as “democratic” and those labelled as “dictatorial” or “authoritarian”. There has always been a particular tension when it comes to the operation of security intelligence agencies since, for example, they are required to act secretly and therefore normal transparency is seen as inapplicable. These tensions came to a head through the 1970s onwards as, in one liberal democracy after another, official enquiries exposed systematic abuses of law and rights that triggered changes aimed at increasing the oversight of intelligence agencies. The wave of democratisations through Central and Eastern Europe and Latin America since the 1980s have led to similar attempts to legalise and democratise intelligence (e.g., Born et al., 2005).

On the face of it, however, 9/11 has brought this welcome process (however uneven and, in some cases, purely symbolic it was) to a grinding halt. Throughout North America and Western Europe, legislation was enacted in the immediate aftermath of 9/11 that sought, in general, to empower intelligence agencies to gather information more easily and to reduce the restrictions that, it was argued, hindered the “war on terror”. For example the USA PATRIOT Act dismantled the so-called “firewall” that was built in the 1970s between information gathered for law enforcement as opposed to intelligence purposes. Non-citizens certified as presenting a threat of terrorism can be detained indefinitely, police and security agencies can gain easier access to electronic communications data and the US Treasury is empowered further to obtain financial information from banks (e.g., Gill, 2004).

In the UK, although a comprehensive Terrorism Act had been passed in 2000 to codify the various measures that had grown piecemeal since the first Prevention of Terrorism Act 1974, the Government still introduced the Anti-Terrorism, Crime and Security Act (ATCSA) 2001. As in the US, this increased “special powers” for the gathering of information *via*, for example, stop and search but also provided for the unlimited detention without trial of foreigners deemed to be a threat (Walker, 2002 for comprehensive discussion). This latter provision required the Government to derogate from the European Convention of Human Rights (ECHR). This is allowed under Article 15 in cases of emergencies “threatening the life of the nation” but it should be noted that the UK alone among European countries has found it necessary to do this. The House of Lords found this section of the ATCSA incompatible with the Human Rights Act in December 2004 forcing the Government to pass the Prevention of Terrorism Act 2005 that includes provisions for “control orders” on those “reasonably suspected”—but not convicted—of being terrorists (Home Office, 2005b).

Germany, France, Italy, Spain and other countries also strengthened their statutory schemes for counter-terrorism in the wake of the 9/11 attacks (DCAF Intelligence Working Group, 2003: 71). The EU responded by implementing more rapidly proposals that were already within the policy making process, for example, the common arrest warrant, and introducing others that had been on the shopping list of member agencies for some time. After the terrorist attack in Madrid on 11 March 2004 the European Council issued a declaration and revised plan of action for member states to pursue. The strategic objectives are: to enhance international efforts to combat terrorism; to reduce terrorists' access to finance; to maximise EU and member state capacity to prevent, detect and prosecute terrorists; to enhance the security or transport and borders; to enhance capabilities to deal with the consequences of attacks; and to address the factors contributing to support for and recruitment into terrorism (www.statewatch.org/news, 26 April 2004).

But new laws do not exhaust the post-9/11 changes—there have also been assertions of new executive power to the effect that previously understood law (and rights) do not apply in the new circumstances. We see a general shift from "national security" as essentially defensive to preventive. It is argued that threats must be countered and suppressed *before* they are imminent. These tendencies actually predate 9/11 as governments characterised problems such as drugs-trafficking, crime and terrorism as "wars" in order to drum up public support and legitimise greater use of pre-emptive means. The increased use of intelligence techniques has very serious implications for rights, for example, the increased use of rendition by the US in which time-consuming extradition processes are by-passed and "suspects" or "enemy combatants" are kidnapped in order to be detained in the US or elsewhere. Since 9/11 rendition has been used to send detainees to countries where torture is in routine use in an attempt to increase the "product" of human intelligence. For example, a Canadian citizen Maher Arar was arrested at JFK and sent to Syria where he was imprisoned for 12 months, suffering torture. The Canadian government has established a judicial inquiry to investigate what contribution the RCMP and/or CSIS made to his rendition (www.ararcommission.ca). It is tempting to see these developments simply as manifestations of the increased transfer of military "war-fighting" techniques into the civilian sphere and there is certainly an element of this (Haggerty & Ericson, 1999; Lutterbeck, 2005) but it should not be assumed that weakening of rights is the responsibility solely of the military. Interestingly, the main opposition to the US's unilateral suspension of the Geneva Conventions regarding the treatment of prisoners and use of torture has come from military lawyers—the legal rationalisation for these policies has been provided by civilian lawyers within the Bush administration (Greenberg & Dratel, 2005).

In the most extreme cases targets are killed: for example the use of "targeted assassinations" by the Israeli Army (IDF) against Palestinians alleged to be "terrorists" since well before 9/11. In the US also, the 1975 prohibition on US agencies engaging in assassinations has been interpreted since 1990 as not applying to "terrorists" but since 9/11 the CIA have been specifically authorised to kill what are described as "high value targets" in the al-Qaeda leadership such as the operation in the Yemen in November 2002 (Risen & Johnston, 2002). Northern Ireland provides many examples of the dangers of uncontrolled military intelligence involvement in counter terrorism. For example, after many years of official denials, inquiries by a Canadian judge and a senior British police officer indicate that state agencies colluded with loyalist paramilitaries in the killing of lawyers and others alleged to be Republicans. Judge Cory's report into the murder of Patrick Finucane, a Catholic lawyer, concluded:

> the documents and statements I have referred to in this review have a cumulative effect. Considered together, they clearly indicate to me that there is strong evidence that collusive acts were committed by the Army (Force Research Unit), the Royal Ulster Constabulary Special Branch and the Security Service. (Cory, 2004: para. 1.293)

Sir John Stevens, then Commissioner of the London Metropolitan Police, found similarly in his own investigation of the murders (Stevens, 2003: para. 4.7)

We have a fairly clear grasp of the mechanisms of accountability as they operate (or not) within the bureaucratic structures of the state: for all their failings as efficient means of service delivery, hierarchies did have the advantage that lines of accountability were clear. To be sure, they could also be highly secretive but, with appropriate access to persons and papers, the possibility of holding people to account was real. We have barely started on the problem of working out means of oversight that are appropriate to rapidly developing and proliferating networks. The answer to the question "Who is to monitor and police informal networks?" (Thompson, 2003: 176) is extremely elusive. For participants, convinced (sometimes with justification, sometimes not) that public safety and national security are in their hands, the very lack of transparency that is afforded by informal networks is their great advantage. People might well decide that the professional risks inherent in security intelligence work are just not worth taking where there is a clearly-documented audit trail leading back to their desk. There is often great scepticism that managers (not all of whom in the military and police will necessarily have intelligence experience) will protect operatives and analysts if a wrong judgement call is made. Power flows are yet more elusive and subtle in networks and traditional forms of inquiry may simply not be appropriate once decisions and knowledge are generated within fluid and flexible networks rather than traditional bureaucracies. Addressing this problem, Sheptycki suggests that networked intelligence "cells" must be organised so that the inefficiencies of hierarchy can be avoided and intelligence shared with the assurance that flows can be audited for compliance with human rights standards such as proportionality (2004: 24–25).

Bayley and Shearing make clear that, if the "public interest" in policing is to be safeguarded, then government must retain the functions of regulation, auditing and facilitation of security networks (2001: 32–33; cf. Button, 2002: 118–130; Caparini & Schreier, 2005).[3] As "policing" becomes firmly embedded within broader networks of security and intelligence, much work remains to develop forms of oversight at least as flexible as the networks for which they are responsible. So, beyond the mapping and explanation of security intelligence networks our final challenge is to investigate ways by which they can be overseen in order to ensure that they are capable of achieving both security and rights.

Notes

[1] "Information" is normally defined as oral, visual or written materials that are gathered or received while "intelligence" is what is produced once those materials have been analysed or evaluated (Gill, 2000: 211).

[2] In the literature on "intelligence", the term is used in a number of closely related ways: to describe a *process*, the *product* of the process and the *people/institutions* who produce it; in what follows the precise sense of the term will, hopefully, be clear from the context.

[3] An interesting example is provided by Portland, Oregon where the Mayor and municipal Police Commissioner insist that they be security cleared to a level that will enable them to oversee the work of their officers involved in Joint Terrorism Task Forces (*Portland Communique*, 23 March 2005).

References

Aldrich, R.J. (2004), "Transatlantic intelligence and security cooperation", *International Affairs*, Vol. 80, no. 4, pp. 731–753.

Andrew, C. & Dilks, D. (eds) (1984), *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*, Macmillan, Basingstoke.

Bayley, D.H. & Shearing, C.D. (2001), *The New Structure of Policing: Description. Conceptualization, and Research Agenda*, National Institute of Justice research report 187083, Washington: Department of Justice, Available online at www.ojp.usdoj.gov/nij (accessed 10 January 2005).

Bichard (2004), *Bichard Inquiry Report*, HC653. Available online at www.bichardinquiry.org.uk (accessed 22 June 2004).

Bigo, D. (2000), Liaison officers in Europe: New officers in the European security field, in: Sheptycki, J. (ed.) *Issues in Transnational Policing*, Routledge, London.

Block, A. (ed.) (1992), "Issues and theories on covert policing", special issue, *Crime, Law and Social Change*, Vol. 18, September, pp. 1–2.

Born, H., Johnson, L. & Leigh, I. (2005), *Who's Watching the Spies? Establishing Intelligence Service Accountability*, Potomac Books, Dulles, Virginia.

Bozeman, A. (1992), Knowledge and comparative method in comparative intelligence studies, in: Bozeman, A. *Strategic Intelligence and Statecraft*, Brassey's, Washington DC.

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

Button, M. (2002), *Private Policing*, Willan, Cullompton.

Buzan, B, Wæver, O. & de Wilde, J. (1998), *Security: A New Framework for Analysis*, Lynne Reiner, London.

Caparini, M. & Schreier, F. (2005), *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*, Occasional Paper, DCAF, Geneva, available online http://www.dcaf.ch/publications/occasional.cfm?nav1 = 4&nav2 = 3 (accessed 8 November 2005).

Carter, D. (2004), *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Michigan State University and US Department of Justice Office of Community Oriented Policing Services. Available online at www.fas.org (accessed 10 January 2005).

Castells, M. (2000), *The Rise of the Network Society*, 2nd edn, Blackwell, Oxford.

"City Sets March 30 Showdown Over Joint Terrorism Task Force", *Portland Communique* (2005), 23 March.

Cory (2004), *Cory Collusion Inquiry Report: Patrick Finucane*, HC470, The Stationery Office, London.

Dandeker, C. (1990), *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Polity Press, Cambridge.

DCAF Intelligence Working Group (2003), *Intelligence Practice and Democratic Oversight—A Practitioner's View*, DCAF, Geneva.

Deibert, R.J. (2003), "Deep Probe: the evolution of network intelligence", *Intelligence and National Security*, Vol. 18, no. 4, pp. 175–193.

der Derian, J. (1992), *Antidiplomacy*, Blackwell, Oxford.

Dorn, N. (2003), Proteiform criminalities: The formation of organised crime as organisers' responses to developments in four fields of control, in: Edwards, A. & Gill, P. (eds) *Transnational Organised Crime: Perspectives on Global Security*, Routledge, London.

Dowding, K. (1995), "Model or metaphor? A critical review of the policy network approach", *Political Studies*, Vol. 43, no. 1, pp. 136–158.

Flood, B. (2004), "Strategic Aspects of the UK National Intelligence Model", in: Ratcliffe, J.H. (ed.) *Strategic Thinking in Criminal Intelligence*, Federation Press, Sydney, pp. 37–52.

Foucault, M. (1991), Governmentality, in: Burchell, G., et al. (eds) *The Foucault Effect: Studies in Governmentality*, Harvester Wheatsheaf, London.

Frances, J., Levačić, R., Mitchell, J. & Thompson, G. (1991), "Introduction", in: Thompson, G., Frances, J., Levačić, R. & Mitchell, J. (eds) *Markets, Hierarchies and Networks: The Co-Ordination of Social Life*, Sage, London.

Giddens, A. (1985), *The Nation State and Violence*, University of California Press, Berkeley.

Gill, P. (2000), *Rounding Up the Usual Suspects? Developments in Contemporary Law Enforcement Intelligence*, Ashgate, Aldershot.

Gill, P. (2004), "Securing the globe: Intelligence and the post-9/11 shift from 'liddism' to 'drainism'", *Intelligence and National Security*, Vol. 19, no. 3, pp. 467–489.

Gill, P. (2004/05), "Policing In Ignorance?", *Criminal Justice Matters*, Vol. 58, Winter, pp. 14–15.

Gimenez-Salinas, A. (2004), "New approaches regarding private/public security", *Policing and Society*, Vol. 14, no. 2, pp. 158–174.

Greenberg, K.J. & Dratel, J.L. (2005), *The Torture Papers: The Road to Abu Ghraib*, Cambridge University Press, New York.

Grieve, J. (2004), "Developments in UK criminal intelligence", in: Ratcliffe, J.H. (ed.) *Strategic Thinking in Criminal Intelligence*, Federation Press, Sydney, pp. 25–36.

Haggerty, K. & Ericson, R. (1999), "The militarization of policing in the information age", *Journal of Political and Military Sociology*, Vol. 27, pp. 233–255.

Hillyard, P. & Gordon, D. (1999), "Arresting statistics: the drift to informal justice in England and Wales", *Journal of Law and Society*, Vol. 26, no. 4, pp. 502–522.

Hoare, O. (ed.) (2002), *British Intelligence in the Twentieth Century: A Missing Dimension?* Special Issue, *Intelligence and National Security*, Vol. 17, no. 1.

Home Office (2004), "Leading the fight against organised crime: Key SOCA appointments announced", Ref: 274/2004, 13 August.

Home Office (2005a), "Bichard inquiry—implementation of recommendations". Available online at www.homeoffice.gov.uk/docs4/bichard_statement.html (accessed 20 January 2005).

Home Office (2005b), Prevention of Terrorism Bill, Background Briefing Papers, February.

Hughes, G. (2000), Communitarianism and law and order, in: Hope, T. (ed.) *Perspectives on Crime Reduction*, Ashgate, Dartmouth.

Hulnick, A.S. (1999), *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Praeger, London.

Intelligence and Security Committee (2003), *Annual Report 2002–2003*, HMSO, London Cm 5837. Available online at www.cabinet-office.gov.uk/intelligence (accessed 15 February 2005).

Johnson, L. (2002), *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*, New York University Press, New York.

Johnston, L. (1992), *The Rebirth of Private Policing*, Routledge, London.

Johnston, L. (2000a), *Policing Britain: Risk, Security and Governance*, Longman, Harlow.

Johnston, L. (2000b), Transnational private policing: The impact of global commercial security, in: Sheptycki, J. (ed.) *Issues in Transnational Policing*, Routledge, London.

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

Jones, T. & Newburn, T. (1998), *Private Security and Public Policing*, Clarendon Press, Oxford.

Jordan, L.J. (2005), "Homeland Security Faces Massive Overhaul", San Francisco Chronicle, June 17, 2005.

Kickert, W. & Koppenjaan, J. (1997), Public management and network management: An overview, in: Kickert, W., et al. (eds) *Managing Complex Networks: Strategies for the Public Sector*, Sage, London.

Klerks, P. (2003), The network paradigm applied to criminal organisations: theoretical nitpicking or a relevant doctrine for investigators?, in: Edwards, A. & Gill, P., *Transnational Organised Crime: Perspectives on Global Security*, Routledge, London.

Knoke, D. & Kuklinski, J.H. (1991), Network analysis: Some basic concepts, in: Thompson, G., et al. (eds) *Markets, Hierarchies and Networks: The Co-Ordination of Social Life*, Sage, London.

Leishman, F. (1999), Policing in Japan: East Asian archetype?, in: Mawby, R.I (ed.) *Policing Across the World*, UCL Press, London.

Lustgarten, L. & Leigh, I. (1994), *In From the Cold: National Security and Parliamentary Democracy*, Clarendon Press, Oxford.

Lutterbeck, D. (2005), "Blurring the line: The convergence of internal and external security in Western Europe", *Security Dialogue*, Vol. 36, no. 1. Available at http://www.gcsp.ch/e/about/News/Faculty-articles/Academic-articles/index-Academic.htm (accessed 15 February 2005).

Lyon, D. (2003), *Surveillance after September 11*, Polity, Cambridge.

McGrew, T. (1992), Conceptualizing global politics, in: McGrew, T. et al., *Global Politics*, Polity, Cambridge.

Manning, P.K. (2000), Policing new social spaces, in: Sheptycki, J. (ed.) *Issues in Transnational Policing*, Routledge, London.

Markle (2003), *Creating a Trusted Information Network for Homeland Security*, 2nd Report of the Markle Foundation Task Force, December, Available online at www.markle.org/downloadable_assets/nstf_report2_full_report.pdf (accessed 15 January 2005).

Marx, G. (1988), *Undercover: Police Surveillance in America*, University of California Press, Berkeley.

Morris, N. (2004), "Secret services to be given access to ID card database", *Independent*, October 28.

Poveda, T. (1990), *Lawlessness and Reform: The FBI in Transition*, Brooks/Cole Publishing Company, Pacific Grove, California.

Risen, J. & Johnston, D. (2002) "Bush has widened authority of CIA to kill terrorists", *New York Times*, December 5.

Schreier, F. & Caparini, M. (2005), *Privatising Security: Law, Practice and Governance of Private Military and Security Companies*, Occasional Paper, DCAF, Geneva, available online at http://www.dcaf.ch/publications/occasional.cfm?nav1=4&nav2=3 (accessed 8 November 2005).

Seifert, J.W. (2004), *Data Mining: An Overview*, Congressional Research Service, Washington, RL31798. Available online at www.fas.org/irp (accessed 16 December 2004).

Shearing, C.D. & Stenning, P.C. (eds) (1987), *Private Policing*, Sage, London.

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

Singer, P.W. (2003), *Corporate Warriors: The Rise of the Privatized Military Industry*, Cornell University Press, Ithaca.

Singer, P.W. (2004), "The private military industry and Iraq: What have we learned and where to next?", DCAF Policy Paper. Available online at www.dcaf.ch (accessed November 2004).

Smith, M. (2003), *The Spying Game: The Secret History of British Espionage*, Politico's, London.

Sparrow, M.K. (1991), "Network vulnerabilities and strategic intelligence in law enforcement", *International Journal of Intelligence and Counterintelligence*, Vol. 5, no. 3, pp. 255–274.

Steele, R. (2002), *The New Craft of Intelligence: Personal, Public and Political*, OSS International Press, Oakton, Virginia.

Stevens (2003), *Stevens Enquiry: Overview and Recommendations*. Available online at www.met.police.uk/commissioner/MP-Stevens-Enquiry-3.pdf (accessed April 2004).

Thompson, G. (2003), *Between Hierarchies and Markets*, Oxford University Press, Oxford.

Thompson, G. et al. (eds) (1991), *Markets, Hierarchies and Networks: The Coordination of Social Life*, Sage, London.

Travers, R. (1997) “The coming intelligence failure”, *Studies in Intelligence*, Vol. 1, no. 1, Available online at www.odci.gov/csi/studies/97unclass/failure.html (accessed 19 February 2002).

Walker, C. (2002), *Blackstones’ Guider to the Anti-Terrorism Legislation*, Oxford University Press, Oxford.

Whitaker, R. (1999), *The End of Privacy: How Total Surveillance is Becoming a Reality*, The New Press, New York.

Web References

www.ararcommission.ca, (accessed 15 May 2005).
www.ci-wackenhut.com, (accessed 15 February 2005).
www.crg.com/html/service_level3.php?id = 362, (accessed 15 February 2005).
www.crg.com/html/service_level3.php?id = 588, (accessed 15 February 2005).
www.fas.org/irp/world/para/scope.htm, (accessed 15 January 2005).
www.group4securicor.com, (accessed 15 February 2005).
www.mpri.com/site/about.html, (accessed 15 February 2005).
www.pinkertonagency.com/global/services.html, (accessed 15 February 2005).
www.securitas.com, (accessed 15 February 2005).
www.statewatch.org/news, (accessed 26 April 2004).