Security Intelligence and Human Rights: Illuminating the ‘Heart of Darkness’?¹

PETER GILL

ABSTRACT Following some democratization of intelligence in the 1990s, the prosecution of the ‘war on terror’ since 9/11 has apparently reinforced the incompatibility of secret intelligence and respect for human rights. The primary reason for this is the changed perception of security risks in the context of a ‘new’ terrorism. The roles of law, rights and ethics in intelligence are discussed with reference to some of the more controversial intelligence activities: informers, interrogation, intelligence sharing, rendition and covert action. Re-invigorated oversight is necessary to protect human rights without hindering agencies’ ability to maintain public safety.

Introduction

We are familiar with civil libertarian concerns about the impact of intelligence activities,² but this article tries to examine more systematically the relationship between intelligence activities, human rights and ethical concerns. This may seem an unpromising venture since, at root, the whole point of intelligence activities is that they ‘require’ actions that infringe on


²‘...mainly secret activities – targeting, collection, analysis and dissemination – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities’: adapted from P. Gill and M. Phythian, Intelligence in an Insecure World (Cambridge: Polity 2006) p.7.
human rights, even if the stated object is the protection of some more or less democratic national security. Much of the information that enters the intelligence process may be from open sources but at some point there is an element of secrecy and the privacy rights of the target are infringed. Traditionally, we would distinguish foreign from domestic intelligence by stating that the object of the latter is to defend the law and uphold the rights of citizens while the object of the former is to break other countries’ laws and infringe the rights of foreigners. Yet, the practices of intelligence are the same and this discussion affects both foreign and domestic agencies.

There has always been controversy about intelligence activities but the context has shifted significantly in the last two decades. Key factors are the establishment of statutory regimes for the conduct and oversight of intelligence, the virtual incorporation of the European Convention on Human Rights (ECHR) into UK law and the implications of the ‘global war on terror’ declared by the US after 9/11. This article discusses this changed context for intelligence intelligence; the place within it of law, rights and ethics; aspects of intelligence practice posing particular threat to rights such as informers and interrogation and, finally, the challenge for intelligence oversight. The important issue of security and rights is now getting more systematic attention although some of the discussion has got bogged down in trench warfare between what Mark Urban describes as ‘human rightists’ and ‘reality checkists’. This labelling should be resisted: democracy depends on rights that cannot be simply ‘traded’ in for the promise of greater ‘security’ and may be upheld as well as threatened by intelligence activities.

The Current Context for Intelligence: Increased Uncertainty

Intelligence is a sub-system of more general social surveillance. We should note that surveillance is not a zero-sum game. On the one hand it is socially embedded: the mentalities, technologies and practices of surveillance are not neutral but are instituted within particular institutional settings;

---

6Gill and Phythian, Intelligence (note 2) pp.29–34.
therefore, they will normally act to reinforce existing power relations. But we should not exclude the possibility that they may act in a non-zero sum way and modify power relations so that the general public interest is enhanced. Therefore, we need to think through the consequences of current intelligence policies, laws and practices. Not all of these have been changed by 9/11 but the context certainly has. Certainly, 9/11 reflected an ‘attack on the United States’ even though it was concentrated in some highly symbolic locations. However, declaring ‘war on terror’ has had some profound consequences, both intended and unintended, though some of the latter were foreseeable. Declaring ‘war’ on a political tactic is not likely to be any more successful than earlier ‘wars’ on drugs or crime. The use of narcotics, deployment of violence for political ends and incidence of ‘crime’ are as old as organized human society and the idea that they can be eliminated by military force, even that of a hegemonic power, is fanciful in the extreme.

Yet it is argued that the terrorism practised by violent Islamists is qualitatively different from earlier forms of political violence – specifically, that it is not ‘negotiable’ in the sense that PLO, ETA and PIRA violence was, but is ‘millennial’, that is, its universal demands are absurd and unobtainable. So, although PIRA violence was presented to the British public at the time as ‘mindless’, crucially, the security authorities knew full well it was not and reacted accordingly. The threat was perceived as essentially a domestic problem, though it did have international implications in terms of fund-raising, acquiring weapons and occasional attacks on service personnel in Germany. However, PIRA was a tightly run, hierarchical organization which, as we now know, was penetrated at a high level. In the early 1980s it was estimated to have about 10,000 sympathizers in Northern Ireland (NI), 1200 of whom would support ‘around 600 active terrorists’. They were concentrated in some areas of the province, though active service units abroad might be more elusive and their modus operandi entailed more risk since those planning attacks wanted to escape and prior warnings were regularly provided, if not always accurate. Finally, their motivation – to drive Britain out of Ireland – was rational, even if unwelcome to the state and government.

Against this picture, the current threat is presented by the UK government as distinctive in four respects: it is an international threat, with suspected terrorists coming from a range of African and Middle East countries, if not actually born in the UK; the threat comes from various individuals, groups and networks, sometimes overlapping to assist each other but independent
of state support; they intend to cause mass casualties and often to kill themselves in the process; and those involved are driven by particularly violent and extreme beliefs. 13 Further, it appears that people may make a rapid shift from ‘sympathizer’ to potential bomber and the profile of those seen as potentially dangerous keeps shifting. Like generals, intelligence analysts are prone to ‘fighting the last war’: after 9/11 the assumption was that the ‘inevitable’ attack in the UK would come similarly from those travelling into the country to carry it out, not from a group born in the UK. After 7/7 greater attention was given to ‘homegrown’ bombers but it is doubtful that the net had spread to include those working as hospital doctors such as those involved in the thwarted attacks in June 2007. At different times, attention has been directed to various places of radicalization – mosques, prisons or gymnasiums – but another aspect of the current situation that is new is the role of the Internet as a source of information and ideas – a very different target from penetrating a branch meeting.

So what is different is the increased uncertainty. Now, while ‘[t]errorism is the politics of uncertainty’, 14 the relative certainty with which government calculated the numbers and identities of PIRA activists has been replaced by glorified ‘guesstimates’. For example, Hennessy reports that by late spring 2005 there were estimated to be 2000 ‘serious sympathizers’ of whom 200 might be prepared to carry out a terrorist attack 15 but another source suggests that by July 2005 the number of ‘primary investigative targets’ known to MI5 had risen from about 250 in 2001 to 800. 16 In a lecture in November 2006 Eliza Manningham-Buller, then Director General of MI5, referred to 200 ‘groupings or networks’ involving 1600 actively plotting or facilitating terrorist acts in UK or abroad, acknowledging ‘many we don’t know of’ and suggesting there could be 100,000 ‘sympathizers’ based on polls of those believing 7/7 bombings were justified. 17 A year later, her successor, Jonathan Evans, spoke of 2000 known to be involved in terrorist activity in the UK, again referring to the probability of as many again who were unknown. 18

This chimes with more general theories of risk society that are concerned with ‘what might happen’ overlaid with higher uncertainties as to precisely what the risk is: ‘The im/materiality and in/visibility of the threats that suffuse the “risk society” mean that all knowledge about it is mediated and

16 J. Bennetto, ‘MI5 conducts secret inquiry into 8,000 al-Qa’ida “sympathisers”’, Independent, 3 July 2006.
as such dependent on interpretation. This is clearly reflected in the intelligence literature to the extent that people have emphasized the centrality of the analysis function; although the main thrust of resource allocation within intelligence still emphasizes gathering. This mismatch is an important symptom of the struggle to match the organization of intelligence to the new conditions and can be accounted for in various ways.

Conceptually, it reflects excessive faith in positivism, that is, the measurement of experiences, preferably quantitative, is at the heart of generating knowledge and it is assumed that more information will reduce uncertainty. Other things being equal, this may be true, but other things are not equal and intelligence’s search for the crucial item of information – the smouldering datum? – that will answer its secrets and mysteries continues to distort the organization of intelligence. For example, two elements of post-9/11 legislation in the US and UK extend both the powers of agencies to collect information and do so on an increased number of actions such as preparation for and ‘glorification’ of terrorism. Individually, these may be sensible steps or they may be the actions of governments terrified at the thought of being accused of inaction but collectively they make the job of agencies in detecting terrorists harder by increasing the net of suspects and adding to information overload. Does the steady increase in the number of suspected attackers referred to above reflect anything more than the increased numbers of MI5 personnel available for surveillance and analysis?

Then there is the ‘political economy’ of intelligence. Just as Dwight Eisenhower warned as he left office of the potentially over-powerful military-industrial complex in influencing US defence and foreign policy, so should we beware of the rapid growth of the security-industrial complex. Of course, this has a number of features including the privatization of war and of policing that involves large numbers of personnel working in the private sector, some on functions formerly conducted by state servants. Yet a very high proportion of the industry is constructed around the development and sale of increasingly complex security technologies. Most of the big breakthroughs in ICT, cryptography, satellite surveillance, detection via sensing (voice, face, smell, etc.) are now made in the private sector. Many are also deployed there but states provide a lucrative market for these systems, even if many are poorly understood. Let us be frank, in a climate of security panic, the search for profits in highly competitive transnational markets leads to the over-selling of various technological ‘fixes’ that fall far short of the advertising.


\[21\] For example, L. Johnston, Policing Britain: Risk, Security and Governance (Harlow: Longman 2000); Johnston and Shearing, Governing Security (note 8).

\[22\] There is an interesting historical parallel. How can we explain the fact that in the mid-1970s many US police forces purchased helicopters? In large part because of the sales effort.
Governments need to reassure their populations that safety and security is their core concern. This is not new – Murray Edelman documented it in his classic *The Symbolic Uses of Politics*\(^{23}\) – but their task is immeasurably harder in the new climate. Significant changes since Edelman first expounded his thesis have, if anything, reinforced it: the neo-liberal hegemony in US and UK since the 1980s is characterized, first, by shrinking the state sector via privatization and, second, by the obsession with performance targets, measurement and the whole panoply of ‘new public management’ (NPM) in what remains of the state sector. Although the numbers employed in intelligence have risen sharply since 9/11, quintessentially, policing and security intelligence never have been concerned with the production of widgets and, as such, their processes may be highly distorted by the reductionism required by NPM. Third, the state’s role as sole security provider diminishes\(^{24}\) just as the significance of security as a political issue has increased. As states seek both to allay and exploit communal feelings of insecurity, the gap between government rhetoric and their ability to actually implement security policies threatens to become so large that it will swallow notions of reasoned proportionality explicit in the human rights discourse that is discussed below.

This has reached its nadir in the ‘one percent doctrine’ attributed to US Vice President Cheney in which the uncertain yet potentially catastrophic nature of the terrorist threat must be ‘prevented’ or ‘pre-empted’ even if there is only a 1% chance of it occurring.\(^{25}\) Put another way, a combination of Rumsfeld’s ‘unknown unknowns’\(^{26}\) and governments’ need to reassure and prove their competence effectively disables traditional calculations of risk. Their need to ‘be seen to do something’ (often by way of legislation) results in policies that, in attempting to deal with threats that are themselves highly uncertain, may not even be implemented or have no measurable impact in terms of increasing security. In a related context of criminal justice policy, Pat Carlen has described this phenomenon as ‘risk-crazed governance’.\(^{27}\) Worst of all, law and policy might actually be counter-productive, that is, provoke ‘blowback’; the experience of discrimination through the enforcement of low-level anti-terrorist powers such as stop and search together with perceptions of egregious repression such as abuse of prisoners may combine to mobilize some people within precisely that population switched to police by helicopter manufacturers whose main market – the Department of Defense in Vietnam – had collapsed.


\(^{24}\) For example, Gill and Phythian, *Intelligence* (note 2) pp.39–61.


group perceived as a threat.\textsuperscript{28} The implication for intelligence activities is clear: they must be conducted legally and ethically, paying due regard to human rights.

**Intelligence: Legality, Rights and Ethics**

As noted earlier, we know that much intelligence is based on open sources. These apparently raise relatively few issues in relation to rights and ethics, though there are some. For example, we can note that the data protection principle still enshrined in legislation in the 1990s that information collected by the state for one purpose could not be used for another has now been swept aside in post-9/11 rush to develop data warehouses that might be ‘mined’ for evidence of suspicious activities (see further below). While it may be the case that this does not raise great moral problems, it certainly does have an impact on the relationship between state and citizen. For example, many post-9/11 legal measures are aimed at increasing the frequency with which citizens have to identify themselves; as Gary Marx observes:

> There is a chilling and endless regressive quality in our drift into a society where a person has to provide ever more personal information to prove that he or she is the kind of person who does not merit even more intensive scrutiny. Here we confront the insatiable information appetite generated by scientific knowledge in a risk-adverse [sic] society. In such a society, knowing more may serve only to increase doubt and the need for more information.\textsuperscript{29}

So, of course, citizens who resist this process will, by the ‘commonsense’ logic of security, render themselves ‘suspicious’ and thus liable to targeting for more intensive surveillance. If citizens will not produce what is required voluntarily, and direct coercion is ruled out, then it must be gathered covertly, which is where intelligence agencies enter the picture. Their distinctive contribution to governance is their covert collection of other people’s secrets.

**Legality**

In the 1970s a series of legislative and judicial developments in North America and Europe instituted a process of ‘legalizing’ intelligence that had previously been subject to executive decrees only. For example, the Canadian McDonald Commission reported in 1981 on inquiries into wrongdoing by the Royal Canadian Mounted Police (RCMP) and


recommended a new legal and organizational structure for security intelligence in Canada, setting out clear principles for the establishment of domestic security intelligence agencies within liberal democracy. Previous to that, Canada, alongside almost all other nations who had established domestic agencies, had done so by executive order in such a way that their actions were technically illegal (notwithstanding debates about the prerogative power) and avoided accountability by means of plausible deniability. McDonald’s basic argument was that, if states believed security threats were so significant as to require special powers for their apprehension, then states must legislate accordingly. This would identify the nature of the powers, the process by which their use could be authorized and a system of oversight by which citizens might reassure themselves against abuse of the powers. The European Court of Human Rights (ECtHR) decision in *Klass v. FRG* (1978) invoked similar reasoning and provided the basis for most subsequent cases and the development of the statutory framework for intelligence activities in the UK. Now the legal context has been enhanced by the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (RIPA) that, essentially, sought to ‘rights-proof’ police and security intelligence procedures in the UK.

In the last quarter-century there has been enormous progress in establishing legal frameworks for intelligence elsewhere as well: in North America and Australasia these were developed in response to intelligence scandals while in Latin America and East and Southeast Europe they have been an important part of ongoing regime change and greater democratization. But while law is a necessary condition for the proper conduct of intelligence, it is not a sufficient condition. Indeed, following McDonald, intelligence law exists largely to authorize intrusion on what are normally considered human rights even if it also establishes procedures to ensure that appropriate authorization is obtained. Thus the law is empowering as well as potentially restricting on the action of state officials.

**Rights**

Nothing in the ECHR limits the ability of states to criminalize particular conduct deemed to be damaging to national security and the ‘margin of appreciation’ permits states discretion in determining how to implement the Convention. The impact in the UK has been mainly on hastening national legislation – the Interception of Communications Act (IOCA), 1985, the Security Service Act (SSA) 1989 and RIPA 2000 – that has, in turn, had most impact on the processes of authorizing intelligence operations rather than


31Conor Gearty suggests that there are three organizing principles by which to ‘make sense’ of the Act and its impact on UK law: respect for civil liberties, legality and respect for human dignity. See *Principles of Human Rights Adjudication* (Oxford: Oxford University Press 2004) p.4. This is a similar perspective to that suggested here for examining intelligence in terms of rights, law and ethics.
preventing agencies from conducting operations they deem necessary. In turn, this is reflected in the increased employment of lawyers within the agencies to advise on operational planning.

Human rights protected under the ECHR are in three categories: absolute, limited and qualified. The main ones affected by intelligence activities are as follows:32

1. **Absolute**: these cannot be restricted in any circumstances, even in wartime or other public emergency, that is, they are ‘non-derogable’. These are the right to life (Article 2) and the prohibition of torture, inhuman and/or degrading treatment/punishment (Article 3). Even though Article 2 is non-derogable, it incorporates circumstances in which states may take life without contravening it, for example, defence against unlawful violence and effecting lawful arrest.33

2. **Limited**: these are derogable ‘in time of war or other public emergency threatening the life of the nation’ (Article 15) but otherwise cannot be ‘balanced’ against any general public interest. These are the right to liberty and security of the person (Article 5), fair trial (Article 6) and freedom of thought (Article 9[1]).

3. **Qualified**: these rights are stated in positive form but also include circumstances in which the general public interest (including national security, public safety, prevention of disorder, protection of the rights and freedoms of others) can be taken into account. These are the right to privacy (Article 8), freedom to manifest religion or belief (Article 9), freedom of expression (Article 10), freedom of assembly (Article 11) and freedom from discrimination (Article 14).

The distinction between these categories requires some discussion of the common rhetorical device that invokes a ‘balance’ between rights and security. The only way to avoid sliding down the endless spiral implicit in Gary Marx’s comment above is to eschew the notion that there is any simple balance between security and liberty, for example, that we can maintain our security if we give up enough rights and liberties. (In fact this is more likely to mean increasing ‘our’ security by reducing the rights of ‘others’.34) Berki

---


33 This was the Article of which the UK was found to be in violation when the ECHR determined that the operation culminating in the shooting of three PIRA members in Gibraltar in 1988 had been badly planned and implemented. *McCann and Others v. UK* (1995); Cameron, *National Security* (note 30) pp.260–62.

pointed to the ‘paradox of security’: the only societies that could guarantee ‘complete’ security either by way of the power of the state or the community would simultaneously be situations of complete insecurity in the face of that all-powerful state or community. Lustgarten and Leigh argued similarly:

if an action taken in the name of national security represses human rights, its justification cannot be established merely by ‘weighing’ the needs of national security against the loss of individual liberty. The loss of liberty must be counted on both sides of the scale and thus deducted from any asserted gain in national security, as well as recognized as a loss to the individuals or groups specifically affected.

Therefore, if there is to be any ‘balancing’ it must be conducted carefully. We must emphasize the respective roles of law, ethics and rights in determining appropriate policies to be implemented to deal with what may, actually, be quite temporary threats. With respect to the first category of absolute rights no balance is permitted, for example, between a perceived security threat and any ‘right’ to torture (cf. the ‘ticking bomb’ scenario and see further below). The circumstances in which the taking of life may not be contrary to the Convention (Article 2[2]) are not an invitation to ‘balance’ but, rather, establish the factual circumstances in which the protection will not apply, for example, defence against unlawful violence and effecting lawful arrest.

Ashworth and Redmayne argue that there is little space for a ‘balance’, either, when it comes to the second group of ‘strong’ rights. Echoing Lustgarten and Leigh, they note the sloppiness of arguments that assume there is no public interest in human rights, merely those of the individual. For example, the ECHR has held that ‘the privilege against self-incrimination could not be outweighed by the social importance of anti-terrorist laws’. Yet they acknowledge that there is a limited space within which competing interests have to be accommodated, for example where ‘public interest immunity’ is claimed in order not to reveal evidence to the defence and the impact of this on the ‘equality of arms’ required by Article 6.

In the third group of ‘qualified’ rights, there is space for ‘balance’ in that Articles 8–11 themselves contain the conditions that may be used to limit the application of rights. For example, with respect to ‘privacy’:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.


2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (Article 8)

But, it is suggested, these provide a particular ‘structure of requirements’ that must be argued if rights are to be limited which is more demanding than any generalized notion of ‘balancing’ security and liberty.39

Again, we might refer to McDonald to establish these requirements or basic ‘principles’ that should underlie any system for the control of information-gathering powers. Bearing in mind that these were to cover domestic, not foreign operations,40 they are:

a) The rule of law must be observed . . .
b) The investigative means used must be proportionate to the gravity of the threat posed and the probability of its occurrence . . .
c) The need to use various investigative techniques must be weighed against possible damage to civil liberties or to valuable social institutions [McDonald had in mind here the potential ‘chilling’ effect of surveillance of political dissent, media etc.] . . .
d) The more intrusive the technique, the higher the authority that should be required to approve its use . . .
e) Except in emergency circumstances, the least intrusive techniques of information collection must be used before more intrusive techniques.41

In the UK these requirements for legality have been met by piecemeal legislation – the IOCA 1985 (legalizing metering and interception of telephone and mail communications); SSA 1989 (providing a statutory mandate for MI5 and authorizing ‘interference with property’ including burglary and theft); the Intelligence Services Act 1994 (similarly establishing and empowering MI6 and GCHQ); and Police Act 1997 (covering, for example, electronic surveillance and ‘interference with property’ by police). Finally, RIPA 2000 was essentially an attempt to codify various surveillance practices and ‘judge-proof’ them from challenge under the HRA.

Detailed research is required to determine the overall impact of these changes. Certainly, human rights are on the intelligence ‘table’ in the way that they were not until the 1970s and there is now a comprehensive legal

39Ibid. p.48.
40Note that the ECHR is also primarily concerned with internal security. Cameron, National Security (note 30) p.53.
framework for the authorization of operations. Thus the law provides a necessary condition for rights-oriented intelligence but it is not sufficient since the law can, in conditions of secrecy, simply provide legal ‘cover’ for abusive practices. Two things are required to prevent this: an ethical framework and a structure for oversight.

Ethics

The ‘rules’ for the conduct of intelligence will be laid down in only the most general way by a statute, ministerial directions can provide more detail but the most detailed guidelines will be written internally to the agency. The enforcement of these rules depends on a combination of training and management but their impact can only be gauged by taking account of their relationship with discretion. Discretion takes different forms but primarily defines that area of choice which is permitted explicitly by the rules, exists by way of the ambiguity inherent in rules or exists simply because of the impossibility of rules anticipating all eventualities. It is a commonplace of organizational theory to note the existence of parallel ‘official’ and ‘unofficial’ structures of power, ‘rules’ and practices. Sometimes these structures will overlap, at others they will conflict. Their interaction will determine what organizations actually do and how they do it: we need to know about the organizational cultures42 that sustain working practices. This is where ethics become crucial.

The view will be strongly expressed that there is no place for ethics in intelligence; commenting on the January 2006 inaugural conference of the International Intelligence Ethics Association, a former CIA officer with long experience said: ‘Depending on where you’re coming from, the whole business of espionage is unethical . . . intelligence ethics is an oxymoron. It’s not an issue. It never was and never will be, not if you want a real spy service.’43 However, if this is viewed as unacceptable, Toni Erskine provides an illuminating summary of how three main approaches to ethics – realist, consequentialist and deontological – might be applied to intelligence activities. She discusses Hobbesian realism that rests on the moral duty of the sovereign to protect her subjects. The resulting argument that intelligence activities are justified if they serve the well-being of the state and nation lends legitimacy to intelligence collection as currently practised. On the face of it there is not necessarily much room here for rights other than that nations might deem it expedient to act with mutual restraint.44

The second approach judges actions by the value of their consequences and, compared with realism, may extend consideration to the interests of people who are neither the target of the act nor the direct beneficiary of the intelligence.

43Quoted in J. Goldman, ‘Ethics Phobia and the U.S. Intelligence Community: Just Say “No”’ in M. Andregg (ed.) Intelligence Ethics (St Paul, MN: Center of the Study of Intelligence and Wisdom 2007) p.17.
those outside the immediate national political community. Here, intelligence activities will be acceptable if they maximize the good through balancing the benefits of increased knowledge against the costs of how it might have been acquired. The difficulty resides in the highly complex computations of goods and harms required in order to draw up Michael Herman’s ‘ethical balance sheet’.\textsuperscript{45} Given what we have said above about rights, clearly a simple utilitarian balance will not do since a notion of the ‘greatest happiness of the greatest number’ would render the rights of minorities irrelevant. Thus, Michael Quinlan argues that, modelled on ‘just war’ theory, ‘just intelligence’ has dimensions both of entitlement to collect information on those who may harm us but also constraint: ‘there are some methods of collection that must never be used’.\textsuperscript{46} As is suggested above, there is a need for ‘structured reasoning’ to ascertain the circumstances under which rights might be infringed in order to achieve a desired outcome.

There is no need for such calculations with Erskine’s third approach – the deontological, where some actions are simply prohibited. Based on the work of Kant, the key principles guiding one’s action are that it might become universally adopted by all other agents and that other people must be treated as ends in themselves, not as tools. Clearly, many intelligence methods, including any deployment of deception and coercion, fail to meet such standards.\textsuperscript{47} These three different positions provide us with clear choices to be made, for example, recruiting and running informers or human sources requires various mixtures of manipulation and deception. For the realist, this will be utilized as long as to do so is in the national interest; for the consequentialist, this will be utilized as long as the benefits of the knowledge outweigh the costs of acquiring it. For the deontologist, however, such methods should not be utilized.

But while it is interesting and important for us to consider these questions in the quiet of the seminar room, it is a very different proposition to see them implemented in the field. Here, I would suggest we just do not have enough systematic knowledge about the way in which intelligence officers carry out their jobs. We have evidence from the abuses at Abu Ghraib and Guantánamo, some at the behest of military intelligence personnel, but there is a pressing need for research, however difficult it will be, in practice, to conduct it. One important hypothesis that we might explore can be derived from what we know about the ‘canteen culture’ in policing and its

\textsuperscript{45}M. Herman, \textit{Intelligence Services in the Information Age} (London: Frank Cass 2001) p.203.


resistance to change. Dominant aspects of this culture include the loyalty to be shown to immediate work colleagues, including concealing their misbehaviours from managers and, even more so, outsiders, the sense of mission that enables individuals to believe that formal rules may be used creatively, bent or broken if the mission demands and possibly racist attitudes deriving from the identity of the ‘usual suspects’. The possibility that these attitudes will be present in the even more secretive and potentially dangerous area of intelligence work seems real. But, for now, let us examine some areas of intelligence practice in which rights are especially vulnerable.

Some Concerns with Rights in the Intelligence Process

The intelligence process is vulnerable at every point to the abuse of rights. Unethical decisions even at the relatively cerebral stages of analysis and policy presentation may result in great social harms, as the determination and presentation of intelligence prior to the invasion of Iraq shows. But some more immediate issues are discussed here.

Targeting

One of the ‘big ideas’ since 9/11 for the prevention of such attacks has been to develop ‘profiles’ of suspects by means of developing data warehouses which link different public and, in some cases, public and private databases, in ways that certainly breach earlier data protection principles aimed at protecting privacy. The most immediate experience of this for most of us is at airports – the US leads the way in developing techniques of behavioural profiling but it is being adopted also by a number of European countries including the UK.

The two core issues are: does it work and is it discriminatory? The first question raises the problem of false negatives and false positives. These systems will ‘work’ to the extent that they identify real security risks who are intercepted or, being known about, dissuade those with violent intentions from pursuing their plans. It is impossible to measure the second and I am not aware of figures published for the first. Arguably, the continued development of these systems has much to do with faith in the technological

---

50 Discussed more fully in Gill and Phythian, *Intelligence* (note 2) pp.125–47.
52 Though we must remember that the then US system identified some of the hijackers on 11 September 2001 for extra screening but they passed it.
fix. Of course, if the profile that selects people for further investigation at airports is deficient then it will not identify those who do pose threats – the false negative.

The answer to the question of discrimination is more complex – basically, of course the system is discriminatory (as is all targeting). The issue is the basis on which the discrimination is exercised – behavioural screening would be consistent with human rights but ethnic profiling would not be unless it ‘is used sensitively and the selection is made for reasons connected with the perceived terrorist threat and not on grounds of racial discrimination’. The problem will often be that behavioural profiling will degenerate into racial profiling which is ineffective because it generates false positives and counter-productive if it reinforces tendencies to alienation.

Gathering

The main impact of Techint is on the right to ‘privacy’ which states might infringe if the conditions of Article 8(2) are not fulfilled. Historically, the UK lost cases under this Article because of the lack of an adequate statutory framework for technical surveillance and a major object of RIPA 2000 was to correct this. The ECHR has developed various general principles, similar to McDonald’s noted above, for interpreting the exceptions to the right of privacy: legality, proportionality, subsidiarity (intrusive techniques must be the last resort), accountability (prior authorization, record keeping and monitoring) and finality (information obtained should be used only for the purpose for which it was obtained).

There are two major issues with Humint: the use of informers and interrogation methods. The asymmetrical nature of terrorism is not just reflected in the nature of weaponry: hi-jacked aircraft, knives, fertilizer truck bombs, etc., but also in the nature of the intelligence contest itself. The interception of communications including mobile phones, e-mail and Internet traffic do have a place within counter-terrorism but can be countered by reliance on personal contacts, frequently changing phones, using hotmail addresses and so on. The lack of human sources within the US communities where the 9/11 hijackers spent time preparing for the attack or the much longer time during which the 7/7 bombers lived and worked in the UK, has led to a belated recognition of the crucial significance for such sources.

However, the use of informers is the most fraught of all information-gathering methods and can raise profound rights issues. The essence of the problem is that informers need to be very close to illegal activities if they are

---

53 Lord Brown of Eaton-under-Heywood in Gillan v Commissioner of Police for the Metropolis [2006] 2 WLR 537 at para.81. This case involved the use by police of stop and search powers under s.44 of the Terrorism Act 2000. Thanks to Ian Leigh for bringing this decision to my attention.

54 See, for example, B. Harcourt, ‘Muslim Profiles Post-9/11: Is Racial Profiling an Effective Counter-Terrorist Measure and Does it Violate the Right to be Free from Discrimination’ in Goold and Lazarus (eds.) Security and Human Rights (note 4) pp.73–98.

to be able to provide useful information. We can identify a series of points where problems arise. Bearing in mind the legality principle, for example, who authorizes them? UK Guidelines for the use of Covert Human Intelligence Sources (CHIS), to give them their official title, are established for ‘public authorities’ in RIPA 2000 and associated codes of practice: for CHIS the Guidelines are very thin compared with those for technical intrusion and authorization only needs to be carried out by organizations themselves. Indeed, authorization of CHIS is not required by RIPA; but if they are not authorized, any resulting evidence might be excluded from a criminal case.\(^{56}\) This will clearly have more impact on police than intelligence agencies but will be an issue to the extent that arrest and charge is the objective of counter-terrorist operations rather than just disruption. However, serious questions need to be asked about actual practices, for example, research into police use of informers during the immediate pre-RIPA period showed that over half of police officers were using unregistered informants; that is, the authorization, recruitment and handling procedures had been by-passed.\(^{57}\)

We have recently received a rare shaft of light into informant handling processes in the context of counter-terrorism from the then Police Ombudsman of Northern Ireland, Nuala O’Loan. As part of her investigation of a complaint about the police’s failure to investigate a murder, she conducted a wide-ranging inquiry into special branch practices in an area of North Belfast. Her findings are chilling, for example:

- failure to arrest informants for crimes to which those informants had allegedly confessed . . .
- the concealment of intelligence indicating that on a number of occasions up to three informants had been involved in a murder and other serious crime; . . .
- creating interview notes which were deliberately misleading; failing to record and maintain original interview notes and failing to record notes of meetings with informants; . . .
- not informing the Director of Public Prosecutions that an informant was a suspect in a crime in respect of which an investigation file was submitted to the Director;
- withholding from police colleagues intelligence, including the names of alleged suspects, which could have been used to prevent or detect crime;
- providing at least four misleading and inaccurate documents for possible consideration by the Court in relation to four separate incidents and the cases resulting from them, where those documents had the effect of protecting an informant; . . .

● giving instructions to junior officers that records should not be completed, and that there should be no record of the incident concerned;  

● destroying or losing forensic exhibits such as metal bars; ...  

● not adopting or complying with UK Home Office Guidelines on matters relating to informant handling, and not complying with the RIPA when it came into force in 2000.  

Now the significance of these points is that they concern counter-terrorist policing in the UK. Clearly, there are differences in the situation in NI from that in Britain with respect to Islamist extremism but we should be alerted to the potential for Humint to involve serious rights abuses.

Regarding interrogation, the post-9/11 controversy concerns the extent to which coercion may be used to gather information from detainees. The ‘ticking bomb’ question moved beyond seminars on ethics into policy discussions. There is not the time to do justice to all the arguments but a few points might be noted. Remembering McDonald’s principles that if states wish to deploy methods that would normally be illegal, then they should legislate for them, it is interesting that Alan Dershowitz’s proposal for ‘torture warrants’ follows the same logic. Dershowitz argued that since, as a matter of fact, states do torture, it would be better to minimize its use by requiring advance judicial authority for its use in certain extreme situations. This would avoid the hypocrisy of plausible deniability after which individuals might face subsequent prosecution for activities to which their superiors had ‘turned a blind eye’. There is a crucial difference between this proposal and McDonald’s in that states are permitted to intrude on privacy and freedom of assembly in the interests of national security and public safety whereas no exception to the ban on torture is permitted. In this respect we must note that the US has distinguished torture from inhuman/degrading treatment in a way that the ECHR does not. Thus ‘enhanced interrogation techniques’ up to and including water-boarding could be conducted ‘lawfully’ because they did not reach the threshold of torture under US law. Even though Congress did outlaw the use of cruel, inhuman or degrading treatment when it passed the Detainee Treatment Act of 2005, it appears that US practices have not been much affected.


However, beyond the legal instruments, there is the issue of ethics. One of the strongest arguments against Dershowitz’s call for torture warrants is the ‘slippery slope’ argument: that, once torture or inhuman treatment is permitted in ‘extreme’ cases, it steadily becomes a new norm. The export of interrogation techniques from Guantánamo is clear and the prisoner abuses at Abu Ghraib were not simply the product of some ill-trained US reservists but were done at the behest of military intelligence personnel, as the first, and best, report on the scandal makes clear. Any claims that torture or ‘aggressive interrogation’ has saved lives must, of course, be subjected to careful scrutiny since the ‘quality’ of information obtained must be highly contested. The debate about rights and the supposedly restrictive mechanisms by which the criminal law seeks to establish the validity of prosecution evidence is, in large part, a way of determining the quality of the evidence and though ‘intelligence’ is judged differently from ‘evidence’, there are very good pragmatic reasons for not beating information out of people. In the longer term, there is the additional factor of the potential blowback – how many potential insurgents and bombers were recruited in Iraq and elsewhere as a result of the broadcast of the shocking images from Abu Ghraib? But, finally, there is the issue of us – what does this do to our image of ourselves as not just upholding freedom and democracy in the world but spreading the word of its advantages to those suffering oppression? As Alex Danchev has argued very powerfully, it is not just the prisoners in Iraq and elsewhere who have been humiliated by US and British forces, so have we.

**Dissemination**

Since 9/11 emphasis has been placed on the need for greater intelligence cooperation, both within and between nations. Within nations this is especially a problem in the US where the extreme fragmentation of the intelligence and law enforcement communities defies comprehension, let alone resolution. Transnationally, there are models, for example, UKUSA, but that was a small and culturally homogenous group of states dealing with a relatively simple perception of ‘the other’ compared to the situation now. No doubt the efficacy of intelligence can be improved in this way though we must note the range of security and other reasons which mean that sharing still tends to

---

62 A. Danchev, ‘Human Rights and Human Intelligence’ in Tsang (ed.) Intelligence (note 4) pp.93–108 at p.107, countering Yoo’s assertion that this argument was ‘hyperbole and partisan smear’, War By Other Means (note 60) p.168.


64 Danchev, ‘Human Rights and Human Intelligence’ (note 62).
be bilateral with those who are trusted rather than more general and multilateral.\textsuperscript{65}

Beyond the practicalities, intelligence co-operation has great implications for rights. The practice of ‘extraordinary rendition’ is clearly based on a desire to avoid the restrictions on interrogation which go with accepted human rights regimes. For example, the case of Maher Arar, a Canadian citizen rendered by the US to Syria where he was detained for ten months and tortured on the basis of inaccurate information from the RCMP has been well documented by a judicial commission.\textsuperscript{66} Jamil el-Banna, resident in UK but not a citizen, was interviewed by MI5 on 31 October 2002 with a view to recruiting him as an informer but gave no indication of wanting to help. The following day el-Banna, Bisher al-Rawi and another man were arrested at Gatwick before boarding a flight to Gambia after a covert search of their luggage found electrical items believed to be suspicious and they were held for three days. When the men were arrested and then released, MI5 sent information to the CIA\textsuperscript{67} about the men but including the caveat that the information was not to be acted upon. Yet, when they did reach the Gambia on 8 November, they were arrested and subsequently passed to the CIA who sent them first to Bagram and then to Guantánamo in February 2003. Al-Rawi was released in March 2007 following UK representations to the US and the evidence strongly suggest he had been a MI5 source for some time prior to his arrest. The great embarrassment of the Security Service at not being able to protect one of their own sources comes through clearly in the Intelligence and Security Committee’s blunt language:

This case shows a lack of regard, on the part of the US, for UK concerns. Despite the Security Service prohibiting any action being taken as a result of its intelligence, the US nonetheless planned to render the men to Guantánamo Bay. They then ignored the subsequent protests of both the Security Service and the Government. This has


\textsuperscript{67}This account is drawn from Intelligence and Security Committee, \textit{Rendition}, Cm 7171, July 2007, paras.111–47. The ISC do not identify the CIA but refer in this part of their Report to ‘US authorities’. Similarly, when the Arar Commission initially published its report, part was redacted. When this was released in August 2007 it was found that the reason for this redaction was that the US had not wanted the FBI and CIA identified as the agencies involved in the rendition of Maher Arar.
serious implications for the working of the relationship between the US and UK intelligence and security agencies.68

**Policy and Covert Action**

The history of British anti-colonialism is replete with examples of covert actions deployed as ‘counter-terrorism’ including the use of ‘counter-gangs’69 in which people from the indigent population were recruited and organized on the basis that it would be easier for them to carry out actions and, of course, they were deniable by the colonial power. So it was in Northern Ireland where, throughout the ‘Troubles’ (1969–97), the apparently random killings of Nationalists by Loyalists and vice versa were routinely presented by government and media as ‘senseless sectarian killings’. Yet, within these respective communities, suspicion grew through the 1980s that many of these cases were not random at all but were the result of co-operation or ‘collusion’ between security forces and paramilitaries.

These concerns reached such a pitch that in 1989, John Stevens, then a Deputy Chief Constable and later Commissioner of the Metropolitan Police, carried out an enquiry that resulted in some prosecutions and reprimands for others but in the conclusion that there was no problem of *systematic* collusion. A second inquiry (also unpublished) took place some years later and then, in May 1999, Stevens was asked to conduct a third enquiry with particular reference to the murder of Pat Finucane in 1989 and a brief report was published in April 2003.70

While Stevens aimed to produce evidence that could be used in prosecution; in parallel, and as a result of the 1998 Good Friday agreement, Canadian Judge Peter Cory was asked to investigate the deaths of two RUC Officers, Bob Buchanan and Harry Breen, Lord Justice Gibson and his wife, Robert Hamill, a young Catholic who was kicked to death by a loyalist mob while armed RUC officers were nearby, Pat Finucane and Rosemary Nelson, Catholic lawyers involved in the defence of people charged with violent offences and Billy Wright, a dissident Loyalist murdered in the Maze prison in 1997. Cory’s mandate was not to make a final determination but to assess whether there was sufficient evidence of collusion as to warrant public inquiries.

Cory defined the problem thus: ‘[Government agencies] must not act collusively by ignoring or turning a blind eye to the wrongful acts of their servants or agents by supplying information to assist those servants or agents in their wrongful acts or by encouraging others to commit a wrongful act.’71

---

68Ibid. para.137.
Judge Cory found evidence of collusion in most cases; in his report into the murder of Patrick Finucane, he concluded ‘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’. Stevens concluded his Third Report into the Finucane and another murder:

there was collusion in both murders and the circumstances surrounding them. Collusion is evidenced in many ways. This ranges from the failure to keep records, the absence of accountability, the withholding of intelligence and evidence, through to the extreme of agents being involved in murder.

If proved, these cases would amount to a clear breach of ECHR Article 2. In five of the six cases he investigated, Cory found that there was enough evidence of collusion to require a public inquiry and in four cases public hearings had begun, or were about to begin, at the time of writing – three to four years after inquiries were announced in 2004. But in the case of Patrick Finucane, a campaign by the family against the restrictions on any inquiry held under the Inquiries Act 2005 led to a stalemate. The campaign received significant support from judges, including Peter Cory, who suggested it would ‘make a meaningful inquiry impossible’.

This might subsequently raise the issue of whether the UK government was in breach of the Article 13 duty to investigate violent deaths caused by state agents although, in 2004, the House of Lords decided this did not apply to deaths occurring, as Finucane’s did, before the HRA came into effect.

The Need for Enhanced Oversight

Hopefully, the import of the foregoing argument is clear. Much progress has been made in recent years in placing intelligence activities on a legal footing. This provides at least the basis for more democratic control of intelligence but law is not sufficient. Indeed, legal structures and authorities may provide simply a superior cloak behind which authoritarian practices continue, so it is crucial to consider the necessary reinforcement of law not only through ideas of rights and ethics but by re-emphasizing oversight.

The current oversight structure in UK has developed piecemeal over the last quarter century – like the law and Topsy, ‘it just growed’ – with a result that seems to some as a triumph for British pragmatism while, arguably, it is a fragmented architecture providing a kind of compartmentalized oversight.

---

73 Stevens, Stevens Enquiry (note 70) para.4.7.
that falls some way short of what is required. Oversight must take place at different levels – internal and ministerial as well as externally. This is necessary in order to achieve compliance with internal guidelines and ministerial directions as well as the law and policy more generally. Parts of the structure are concerned only with compliance with law – for example, the UK commissioners and tribunals have a mandate to apply the principles of judicial review in overseeing the issuing of warrants and investigation of complaints of improper surveillance. This erects a minimal standard of legality for the actions of the agencies that takes insufficient account of crucial ethical issues.

The strongest trend in intelligence oversight in recent years, however, has been the establishment of parliamentary committees or, as in the UK, a ‘committee of parliamentarians’. There has been a small rush of studies recently published, reflecting on the first ten years of the Intelligence and Security Committee’s (ISC) existence which broadly agree that the ISC represents an important innovation in the governance of UK intelligence that established some early credibility but which has been reduced because of its rather supine performance over Iraqi WMD. Various suggestions have been made for improvement, for example, that the committee’s chair should be a member of the opposition, that they need more staff, that it should hold hearings in public where classified information is not to be discussed and that it should be less accommodating to government requests for the redaction of material from its reports.

However, the main point I want to make is that the ISC should place the issue of human rights at the centre of its work. Arguably, the ISC has allowed itself to spend too much time on managerial matters – resource allocation (IT systems such as SCOPE, buildings, etc.). It is not that these things are unimportant, it is just that parliamentary oversight is responsible for much more than acting as management consultants for the government. None of its reports before 2005 made any explicit reference to human rights at all, which seems remarkable given the concerns with intelligence activities prompting the introduction of oversight in the first place. Since then, two ISC Reports have dealt with rights issues. However, when they dealt with the issue of prisoner abuse in their report in March 2005 the committee did little more than repeat the agencies and ministers’ utilitarian justifications for compromising with the US and using information obtained under torture. This is not good enough. The ISC mandate is to oversee the ‘expenditure, administration and policy’ of

---

76 Gill and Phythian, Intelligence (note 2) pp.148–71.
78 Intelligence and Security Committee, Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantánamo Bay and Iraq, Cm 6469, March 2005, and see Gill, ‘Evaluating Intelligence Oversight Committees’ (note 77) pp.26–7.
the agencies which are ‘public authorities’ in the terms of the Human Rights Act and their compliance requires close scrutiny.

In July 2007 the ISC published the report of its inquiry into allegations that UK agencies had been involved in US policies of rendition.79 It paints a picture of a slowly dawning realization in the UK agencies as to what the US was actually doing so that, after 2003, ministerial authorization was routinely sought whenever it was feared that intelligence provided to a third country – not necessarily the US – might lead to a rendition. It concludes that the UK agencies did not knowingly collude in extraordinary rendition and, as we saw above, was very critical of the US ignoring the normal rules of intelligence sharing. However, questions remain. For example, their investigative resources are minimal80 and so, if we ask: ‘how does the Committee know that the UK agencies did not knowingly assist any rendition where there was a real risk of someone being tortured or subjected to cruel, inhuman or degrading treatment?’, the answer is because the Permanent Secretary for Intelligence, Security and Resilience says so, based on inquiries by the agencies, including a questionnaire to staff.81 Now, this specifically related to the period before 9/11 but, given the pressures on the agencies thereafter and the poor record keeping noted by the Committee, they do not seem to have been able to carry out any more thorough investigation for the period after 9/11. Given the history of intelligence oversight, it is not simply cynicism which leads to the conclusion that this is not good enough.82

While it may be the case that oversight committees can never guarantee that intelligence (or any other) state agencies will not abuse their powers and the rights of citizens, parliamentary oversight must be conducted in the realization that where people believe they are acting in the interests of national security they will mislead oversight bodies including courts. In the trial of Brian Nelson for offences committed while he was UVF intelligence officer and an informer, Colonel Kerr (at the time of the trial identified only as Colonel ‘J’) appeared for the defence and told the court Nelson had been responsible for saving 200 lives – he lied. Stephens’ investigators later said the number was probably two – one of whom was Gerry Adams.83 Around the same time, remember, so anxious were military intelligence to derail Stevens’ investigations of collusion that they warned Nelson of his impending arrest and, when Stevens rearranged the operation, his incident

---

79 Intelligence and Security Committee, Rendition (note 67).
80 Aggravated by the decision not to appoint a new investigator after the sacking of John Morrison.
81 Intelligence and Security Committee, Rendition (note 67) paras.46–8.
82 One specific loose end left by the ISC concerns Diego Garcia. They report that the PM told them that the US had given ‘firm assurances’ that no-one had been held on Diego Garcia (Intelligence and Security Committee, Rendition (note 68) para.197). The Foreign Affairs Committee investigated further and concluded ‘that it is deplorable that previous US assurances about rendition flights have turned out to be false’ (Foreign Affairs Committee [Overseas Territories], HC 147, July 2008, para.70).
83 J. Ware, ‘A Licence to Murder’, Panorama, BBC1, broadcast 18 and 23 June 2002.
room was destroyed by what he believed was a deliberate act of arson.\(^{84}\)

More recently, reflecting on her investigations in North Belfast, the Northern Ireland Police Ombudsman, Nuala O’Loan, reported:

> Some retired officers did assist the investigation, and were helpful ... Others, including some serving officers, gave evasive, contradictory, and on occasion farcical answers to questions. On occasion those answers indicated either a significant failure to understand the law, or contempt for the law. On other occasions the investigation demonstrated conclusively that what an officer had told the Police Ombudsman’s investigations was completely untrue.\(^{85}\)

And obstruction continues: in the early stages of the public inquiries into collusion in the murders of Rosemary Nelson, Billy Wright and Robert Hamill, the Ministry of Defence and Security Service among other government agencies were demanding the return of secret documents from the Stevens inquiry. In some cases they were sent only to be destroyed so the Stevens investigators – likely to be called as witnesses to the inquiries – had taken to copying those that were returned.\(^{86}\) On the opening day of the hearings in the Wright inquiry, lawyers outlined their problems in obtaining key files from government agencies. The lawyer for the Wright family told the inquiry that thousands of prison documents and journals had been destroyed and the lawyer for the Inquiry itself said it had ‘experienced difficulties’ in obtaining documents including delays and gaps in what was provided by Police Service of Northern Ireland, prison authorities and the Security Service.\(^{87}\)

There is a large area of discretion available to intelligence agencies as to how they do their work and organizational cultures are crucial in determining how that discretion is exercised. Of course, no oversight committee has the resources to monitor all aspects of the agencies’ operations but there are some key areas to which attention should be paid and the Brown era discussion of the status of the ISC must include the issue of staffing. Recruitment, training, codes of ethics, international co-operation and the challenge of security networks beyond the state are all issues requiring attention. If left simply to ‘insiders’, the issues may be dealt with from the mindset of law and rights as minimal standards for practice or, worse, as minimal standards for reporting on practice.

**Conclusion**

There is currently great pressure on government and security authorities to provide public safety in the context of heightened uncertainty as to precisely

\(^{84}\) Stevens, *Stevens Enquiry* (note 70) para.3.4.


the size and source of the terrorist threat. The task is to ensure that their efforts do not themselves undermine democracy and the rule of law as much, if not more, than the threat itself. Therefore, the actions of intelligence agencies must be scrutinized since they act in our name. Literature provides for even more ambiguity than the law and one interpretation of what Kurtz meant when, just before his death in Africa, he intoned ‘The horror! The horror!’ is that he was passing moral judgement on his own actions.88 At the end of Conrad’s story, with the return of Marlow, his narrator, to the Thames, it is clear that the ‘heart of darkness’ is neither something ‘past’ nor ‘other’; rather, it ‘is located at the heart of the “civilizing” mission’.89 Illuminating this darkness is the challenge for intelligence oversight.

89 Ibid. p.xxxiv.