Intelligence and National Security

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fint20

Intelligence, Threat, Risk and the Challenge of Oversight
Peter Gill
Published online: 27 Apr 2012.

To cite this article: Peter Gill (2012): Intelligence, Threat, Risk and the Challenge of Oversight, Intelligence and National Security, 27:2, 206-222
To link to this article: http://dx.doi.org/10.1080/02684527.2012.661643

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.tandfonline.com/page/terms-and-conditions

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae, and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
Intelligence, Threat, Risk and the Challenge of Oversight

PETER GILL*

ABSTRACT Intelligence studies has traditionally talked in terms of ‘threats’ though the idea of ‘risk’ has now entered its language, as it has so many other areas of policy. The key distinction remains the notion of threat of intentional action to cause harm: this is the central preoccupation of intelligence agencies that would not normally consider risks that might arise from, say, the unintended outcomes of accidents or interrupted supplies of resources. Another distinction is that intelligence is normally preoccupied with increasing knowledge in conditions of ignorance or uncertainty, while risk analysis is more likely to be quantifiable. The perception of a ‘new terrorism’ has led to the importation of the ‘precautionary principle’ to intelligence with potentially dangerous consequences for democracy. This requires enhanced thinking and practice with respect to the oversight of intelligence activities, especially in developing security networks.

Introduction

Students of ‘intelligence’ and ‘risk’ have always occupied similar territories but did not normally acknowledge the fact, partly because they tended to use different vocabularies to describe their fields of interest – the former concentrated on security ‘threats’ and the latter on safety ‘risks’. As we shall see below, there remains a key distinction but over the last 20 years these fields have converged for several reasons including the proliferation of asymmetrical threats and broadening of the concept of security beyond the ‘national’ to a broader array of ‘human’ concerns.¹ This article discusses the implications of these changes for the interconnections between intelligence and risk. These questions can be studied at various social ‘levels’ from the macro to the micro: the concentration here is on the organizational level, though it discusses some more general implications for governance.

*Email: p.gill@liv.ac.uk

What is Intelligence?
Specifically, intelligence is:

mainly secret activities – targeting, collection, analysis, dissemination and action – intended to enhance security and/or maintain power relative to competitors by forewarning of threats and opportunities.²

‘Intelligence’, as Kent pointed out, may also be taken to refer to those organizations that carry out these activities and to their ‘product’.³ But, in all cases, the knowledge/power connection is axiomatic⁴ and in order to distinguish intelligence from a myriad of other ‘knowledge management’ practices, note that its object is security, some element of it will be conducted in secrecy and, because it is always relative to others, it will provoke resistance.

What is Risk?
A recent survey of the vast risk literature concludes that the following is the most useful definition of risk:

Risk is defined as the answer to three questions:

1. What can happen? (i.e. what can go wrong?)
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?⁵

Threats, Risk and the Quality of Knowledge
Intelligence studies has traditionally talked in terms of ‘threats’ (emanating from intentional actions) though the idea of ‘risk’ has now entered its language, as it has so many other areas of policy. This means that the terms ‘threat’ and ‘risk’ are now often conflated or some might distinguish between a ‘safety’ risk of accidental harm and a ‘security’ risk of intentional harm.⁶ For example, the UK government has issued a ‘National Security Risk

Assessment’, allocating 15 ‘risks’ to three tiers of priority but only four are not traditional ‘threats’ involving intentional action: a major accident or natural hazard such as severe flooding (tier 1); non-deliberate disruption to satellite information (tier 2); and accidental disruption of fuel supplies or essential resources (tier 3).\(^7\) We see in this example of an ‘all hazards’ approach that policymakers and emergency planners seeking to prevent social harm may well find the distinction unhelpful. Indeed, ‘intentionality’ is not the sole criterion in allocating legal responsibility for causing harm: the cash-strapped manufacturer may not ‘intend’ harm by disposing illegally of hazardous waste but her action will incur liability since the harm could be foreseen and probably breaches regulations.

Yet, within the profession of intelligence it would still be normal to concentrate on threat analyses of, for example, opponents’ capabilities and intentions, to which we might add opportunity, will and potential for impact.\(^8\) Is the threat/risk distinction useful or might it be abandoned? We are most familiar with risk in terms of its calculability, for example, with ‘normal’ diversifiable risks the insurance industry works with the law of large numbers to calculate risks and premiums. Other versions of quantitative risk assessment (QRA) were developed for assessing risks of rare but high consequence in technological systems but these are very different from the human ‘systems’ with which intelligence is concerned. John Garrick, however, maintains that QRA can be useful for managing acts of terrorism, albeit the first question would need to change from ‘What can go wrong?’ to ‘How can I make something go wrong?’\(^9\) But introducing intentionality into QRA produces a qualitative, not just quantitative change and, at the very least, ‘strains the capacity of quantitative risk analysis’.\(^10\)

Others have put the case more strongly: ‘new terrorism’ is so much more lethal and unpredictable that governments have no choice but to prevent or pre-empt it (see further below). What some have described as the politicization of the precautionary principle was most clearly demonstrated in the 2003 Iraq invasion.\(^11\) Developed initially in the health and environment fields, the principle is that uncertainty is no excuse for inaction against serious or irreversible risks and that the burden of proof that an activity or product is safe will be shifted to its sponsor if it is not to be


banned.\textsuperscript{12} Such was the position of the US and UK governments following 9/11, shifting the burden of proof to ‘rogue’ states to show that they did not harbour weapons of mass destruction or terrorist cells, or else face attack.\textsuperscript{13} This is the central cause of the convergence of threat and risk analyses that requires examination. On the face of it, since security intelligence and ‘high policing’ have always been based on a logic of prevention, this actually requires little change in the intelligence process itself, at least up to the point at which action is contemplated. We shall return to the implications of this below but, first, discuss how the quality of knowledge relates to assessments of probability.

In summary, as represented in Figure 1, the central argument is that threat assessments produced by intelligence agencies and risk assessments produced by business or health agencies all attempt to calculate probabilities multiplied by harm. The difference between them is that threats are defined as explicit intentions to cause harm while risks are events that would cause unintentional harm.\textsuperscript{14} In considering ‘probability’, the following description of varying ‘qualities’ of ‘knowledge’ and their implications for action or the exercise of power is useful:

In the case of (a decision under) certainty we know the outcomes of different choices and the only challenge is to be clear about one’s preferences. In the case of risk we know the outcomes (benefits and adverse effects) and the probability of various outcomes. In the case of uncertainty we know the possible outcomes but have no objective ground to estimate their probability. In the case of ignorance we do not even know what adverse effects to anticipate or we don’t know their magnitude or relevance and have no clue of their probability.\textsuperscript{15}

These can be visualized along a continuum; if ‘certainty’ has been established there is no further need for ‘intelligence’ as such but it becomes increasingly significant – and difficult – the nearer we move


\textsuperscript{14}There is one obvious point at which ‘risk assessment’ is central to intelligence operations and that is in respect of calculating risks to safety of operatives, agents and others when planning specific operations. David Strachan-Morris discusses this in his article.

towards ‘ignorance’. Traditional risk analysis has operated mainly in the first two conditions (certainty and quantifiable risk), whereas intelligence has always operated primarily in the other two (ignorance and uncertainty). The overlap occurs in ‘uncertainty’ where quantification is impossible and the precautionary principle may come into effect. ‘Harm’ summarizes the variety of factors involved in estimating potential damage including perceptions of vulnerability, resilience and the ‘appetite’ for risk.

**Figure 1. Threat, Risk, Probability and Harm.**

Threats in the Intelligence Process

What do intelligence experts and organizations actually do when they deem something more or less threatening or dangerous?

**Planning or Targeting**

This is a crucial yet often overlooked issue because otherwise information overload is the only outcome of the intelligence process. Governments and agencies will deploy various means to try to deal with the issue of priorities, for example, the UK Joint Intelligence Committee sets ‘requirements’ and agencies establish more specific targets. The problems involved intensify the greater the uncertainty; no agency outside of a counterintelligence state will have sufficient resources to monitor all perceived (and imagined) threats. Normal methodology is based on the networks of those already known but, of course, this runs the risk of missing completely the ‘clean skin’ or group that has evaded notice. Profiling is a current technique for identifying ‘threats’ from the analysis of aggregate data but is prone to error in terms of
producing both ‘false positives’ and ‘false negatives’. The former may result in discrimination which itself can ‘blowback’ by alienating the very communities whose cooperation is required to provide relevant information. The latter will occur to the extent that the profile is inaccurate: one key difference in counter-terrorism from conventional risk analysis is that the subjects resist surveillance and may change their behaviour or practice deception.

Gathering

Open sources plus scientific enquiry will be at the heart of gathering information on risks and provide much information also on threats at the strategic level but the distinctive contribution or ‘value added’ by intelligence comes as a result of covert intelligence gathering. Its object is both to outwit secrecy and unravel ‘mysteries’ but it is not simply a technical question of whether it can provide answers but, by having some impact on the target and sponsoring resistance, it may itself change the very dimension of the threat, either increasing or decreasing it. Thus information gathering itself should be subject to a risk analysis not only in terms of the safety of people doing it but also its foreseeable impact.

Analysis

What does information gathered actually mean? Here, there is a direct equivalent with what Hutter and Power describe as the ‘sense making’ that is at the heart of organizational encounters with risk.\(^\text{16}\) There is no need to get hung up on a dispute between realist (objective dangers exist out there...) and constructivist (the perception of any danger is a social construction...) approaches to risk; intelligence works (we hope) on the basis of identifying actual rather than imagined dangers but needs to be constantly alert to the importance of assessing them realistically.

Bruce and George identify three broad types of analytical error:

i) through ambiguous, deceptive, contradictory and missing information;
ii) through ‘mindset’, faulty assumptions, poor tradecraft or epistemology;
iii) through policy bias, adoption of policymaker biases or politicization.\(^\text{17}\)


The analytical problem may be simplified for those who maintain that QRA can be applied to counter-terrorism but the argument here is that intelligence operates where QRA is, by definition, unavailable. As we have seen, the potential for a risk insurance approach is undermined by the grave and irreversible damage envisaged, aggravated by the uncertainty as to what might happen in the future, the capacity of analytical techniques and the effects of any subsequent action.

**Dissemination**

Different consumers require different types of product, for example, there is an important difference between tactical counter-terrorism, ‘warning’ intelligence, and strategic foreign intelligence. The central problem here is how analysis can convey a necessary sense of uncertainty in the risk calculation without alienating those whose job it is to determine appropriate action. So, given that executives who must act crave certainty, analysts face the apparent paradox of requiring a more precise analysis while at the same time demanding more confidence in the results. This places great demand on the presentation and communication of uncertainties.

While it is understandable that people call for quantitative methods to be developed further so that they can play a greater role in preventing surprise attacks, it raises the danger that ‘certainty’ may be wrongly imposed on uncertainty in order to meet customer demand. The search for ‘truth’ in intelligence is praiseworthy and accounts for the dominance of positivism within intelligence but it may be highly misleading – the more so the greater the complexity and uncertainty of the threat being assessed.

**Action**

In all fields, organizations are both producers and managers of risk. Action/policy feeds back, even gathering may have impact on target and sponsor resistance. Where we see the conventional relation of knowledge informing policy then the nature of ‘policy’ will be crucially affected by the degree of certainty regarding the accuracy of the ‘intelligence’, for example, the Clinton administration’s response to the attack on USS *Cole* in October

---

18E.g. Garrick, ‘Perspectives on the Use of Risk Assessment to Address Terrorism’.
21For example, Uzi Arad, ‘Intelligence Management as Risk Management: The Case of Surprise Attack’ in Bracken, Bremmer and Gordon (eds) *Managing Strategic Surprise*, pp.43–77 at p.76.
22Ambiguities in language may very understandably lead to the quantification of estimates of probabilities but these may be just as misleading.
23Hutter and Power, ‘Organizational Encounters with Risk’, p.3
2000 was limited because the CIA was unable to present anything beyond a ‘preliminary judgment’ that Al Qaeda directed the attack.  

Just as we have seen that there is a continuum of our confidence in the quality of our knowledge from ignorance to certainty, so there is in the terms applied to subsequent action. For example, the greater the degree of uncertainty the more likely it is that regulation will be ‘precautionary’ rather than ‘preventive’. There is a parallel distinction in the notions of preventive and pre-emptive war, the former being more aggressive and anticipatory without an imminent threat and the latter involving an imminent (and thus more certain) threat. We can identify a similar continuum in the domestic arena in relation to suspected terrorist activity: uncertainty leads to prevention/disruption; ‘reasonable suspicion’ to arrest; likelihood of conviction to prosecution; and ‘proof beyond reasonable doubt’ to conviction.

Assessing the Terrorist Threat

Now, ‘(t)errorism is the politics of uncertainty’. As we have seen, intelligence has always worked predominantly within the ‘uncertainty’ segment of the ‘probability’ continuum but there is a realization of its greater depth: we are uncertain not just about the presence or location of a threat and the extent of its consequences but also about the efficacy of our methods for assessing it. This can be illustrated by comparing the official UK perception of the threat posed by the Provisional Irish Republican Army (PIRA) with that since 9/11. The relative certainty with which government calculated the numbers and identities of PIRA activists has been replaced by glorified ‘guesstimates’ of Al Qaeda in terms of its nature, form and strength. (There is disagreement as to extent of similarity/dissimilarity between Northern Ireland and the current situation; my point is the official emphasis on dissimilarity.)

The PIRA threat was perceived as essentially a domestic UK problem, though it did have international implications in terms of fund-raising, acquiring weapons and occasional attacks on service personnel in Germany. Yet, 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, 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, but their *modus operandi* entailed more risk for them because those planning attacks wanted to escape and prior warnings were regularly provided, if not always accurately. Finally, their motivation – to drive Britain out of Ireland – was rational, even if unwelcome to the state and government. Thus, even if the Northern Ireland violence was presented to the British public as ‘mindless’, crucially, the security authorities knew full well it was not and reacted accordingly. How else can we account for MI6 personnel maintaining ‘back channels’ to PIRA through some of the worst periods of violence or the fact that a peace settlement was eventually reached?

By comparison, 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 United Kingdom; 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.29 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.

Peter 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.30 In December 2007, Jonathan Evans, Director General of MI5, spoke of 2000 known to be involved in terrorist activity in the United Kingdom, and, crucially, referred to the probability of as many again who were unknown31 and just over a year later said ‘We don’t have anything approaching comprehensive coverage’.

In 2010, Evans reiterated the point about necessarily allocating priorities to investigations, thus implying that coverage remains far from complete but would not give specific figures: ‘I don’t want to give a number for those of current security interest as that has sometimes been used in the past as a kind of metric for the severity of the threat.’33

33Address at the Worshipful Company of Security Professionals by the Director General of the Security Service, Jonathan Evans, 16 September 2010, Evans also said: ‘In recent years we appear increasingly to have imported from the American media the assumption that terrorism is 100% preventable and any incident that is not prevented is seen as a culpable government failure. This is a nonsensical way to consider terrorist risk and only plays into the hands of the
Countering the Terrorist Threat

So, how is ‘knowledge’ of terrorism translated into action? Michael Warner has drawn on the literature of risk and uncertainty to illuminate the link between knowledge and power. He characterizes intelligence as ‘risk shifting’, showing how ‘sovereignties’ seek to distribute their risk and uncertainty outward, some of it by increased cooperation with allies and some by imposing it on adversaries. But when uncertainty darkens towards ignorance, this process may simply collapse knowledge into power. Ron Suskind reports the White House meeting in November 2001 that discussed the possibility of Al Qaeda obtaining a nuclear weapon from Pakistan at which the vice president proposed:

If there’s a one percent chance that Pakistani scientists are helping al Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response … It’s not about our analysis, or finding a preponderance of evidence, it’s about our response.35

Even if Suskind’s sources were not precisely accurate, what became known as the ‘Cheney Doctrine’ provides an appropriate metaphor for a condition of almost perfect ignorance – 1 per cent of ‘knowledge’ – as the basis for action. Here we see the result of a political and psychological dynamic of fear and dread set in train in the United States by 9/11 that results in an Iraq-style fiasco in which power/policy determines what is ‘knowledge/ intelligence’ and where knowledge collapses into power.

What happens whenever security fears combine with governments’ attempts to provide reassurance and dominate politics? The lethal combination of uncertainty bordering on ignorance and governments’ urge to act can require steady increments of law; the United Kingdom in the first decade of the twenty-first century is a prime example as each attack apparently demonstrated the inadequacy of previous measures. Given the catastrophes envisaged, and the inevitability of failures of intelligence, there is almost no limit to the measures envisaged and no real evaluation of the actual outcomes of previous policies. In the related context of UK criminal terrorists themselves. Risk can be managed and reduced but it cannot realistically be abolished and if we delude ourselves that it can we are setting ourselves up for a nasty disappointment’. <https://www.mi5.gov.uk/output/the-threat-to-national-security.html> (accessed 17 January 2011).

justice policy 1997–2007. Pat Carlen has described this phenomenon as ‘risk-crazed governance’.38

Thus intelligence is not just linked intimately with power,39 it may actually become a form of governance itself. Even its most passive actions implicate intelligence in governance; therefore it is never enough to view intelligence as just a form of ‘staff’ to ministers and governments. Consequently, intelligence studies must make as much use of theories of power as of theories of knowledge and risk. We need to specify how the intelligence–power relationship defines the state in general. As we know from the literature, a broad distinction has often been drawn between ‘counterintelligence states’40 in authoritarian regimes and those in democracies, but a more nuanced approach is required. For some time we have sought to distinguish states in terms of the degree of influence or control in politics enjoyed by those in security roles. As this increases then we have been more likely to talk about ‘(national) security’ or ‘garrison’ states.41

While some have argued that 9/11 has shifted the balance toward the security or surveillance state,42 others have taken a more benign view and characterized the situation, at least in the United Kingdom, as a ‘safety state’43 or ‘protective state’44 on the grounds that, while it may have accumulated more security powers, it has done so with a greater degree of openness than during the Cold War. In the United States, on the other hand, it is argued by Tim Shorrock that an intelligence–industrial complex has been born in the United States from a blend of patriotism, national chauvinism, fear of the unknown, and old-fashioned war-profiteering.45 What is striking about this is, of course, that public–private contracting and

---

44Hennessy, The New Protective State.
partnership are facts of any liberal capitalist economy, but the *merging* or *symbiosis* of interests in security and intelligence apparatus takes us into the realms of a corporatist state in which government takes place *through* private corporations. This raises profound issues about the nature of intelligence governance.

**Intelligence, Threats, Risk and the Challenge for Oversight**

In the last 30 years or so considerable progress has been made towards establishing the principle that intelligence activities must be subject to democratic control and oversight, even if only a minority of nation states have actually started taking practical steps to achieve it. The objective of intelligence oversight is to increase both its efficacy and propriety. In terms of our ‘probability’ continuum, the object of intelligence is to shift the state of knowledge from ignorance towards certainty or, as practitioners would say, ‘truth’.46 Whether or not intelligence is effective in doing so varies widely in time and place; the answer is always contingent. Oversight becomes even more crucial with the importation of the precautionary principle into intelligence because actions may not only abuse rights but also increase the threat. Law and policy might actually be counterproductive, that is, provoke ‘blowback’; for example, the experience of discrimination through the enforcement of low-level anti-terrorist powers such as stop and search together with knowledge of egregious repression such as abuse of prisoners (as at Abu Ghraib) may have combined to mobilize more people within precisely that population group perceived as a threat.47 The leaked joint Foreign and Home Office study of 2004 provides evidence for this in respect of UK counter-terrorism policies, Iraq and Afghanistan.48 But this is not a necessary outcome; if threats are assessed correctly and attacks thwarted, then intelligence succeeds.

Outside of terrorism, there are other areas where covert methods are necessary in order to examine corruption, white collar, and organized crime including the trafficking of arms and people. Intelligence personnel provide ‘back channels’ in peace negotiations, imagery intelligence (IMINT) analysis was used for the location of mass graves in Bosnia, satellite photography can observe population movements brought about by government or militia

46This is not just to assess the ‘threat at hand’ but also explore other possibilities beyond security *threats*; for example, our earlier definition referred also to seeking *opportunities*, especially economic within a competitive global economy.
attacks on civilian populations in inaccessible areas and map climate change, and so on. There are great possibilities but a note of caution must be sounded: there are many areas of social policy such as health and education where information analysis in the broadest sense is key but in which it makes no sense to involve the ‘spooks’. Thus, intelligence can advance human security but the role of oversight remains to ensure that intelligence is conducted proportionately, not to seek some mythical ‘balance’ between rights and security.

After many years of benign neglect, states have, in the past quarter of a century, started to get to grips with the issue of oversight of intelligence agencies but those efforts have, so far, been based on conventional notions of oversight of state hierarchies in which lines of formal authority are clear, thus making the job of external audit and oversight at least comprehensible, if still devilishly difficult in practice. But these procedures have all been adopted within different national intelligence systems and are restricted to oversight of state intelligence agencies. National overseers lack authority outside their own country and, indeed, the ‘3rd Party rule’ inhibits oversight even within countries.

But intelligence is an activity conducted also by many more or less formal organizations outside of states and the interconnection between these provides fresh challenges. Networking between state agencies and the interpenetration of ‘sovereign’ (e.g. Awakening, Hezbollah, other militia or paramilitary groups), corporate and state intelligence sectors increases in significance. However we characterize ‘risk-shifting’ between, say, state and corporate sectors – as nodal governance, symbiosis, corporatism or as a return to feudalism – we shall face the problem of oversight.

The extent of the problem has been amply illustrated by the US policy of ‘extraordinary rendition’ involving ‘extra-judicial transfer ... for the purposes of detention and interrogation ... where there is a real risk of torture or cruel, inhuman or degrading treatment.’ There had been occasional ‘renditions to justice’ for many years, mainly by police agencies close to


\[50\] Using Mike Warner’s term for groups who are neither state nor corporate but who are willing to use violence in defence or advancement of their political, social or economic interests. Warner, ‘Intelligence as Risk Shifting’.


\[52\] Shorrock, Spies for Hire.


\[55\] Intelligence and Security Committee, Rendition, Cm 7171, July 2007, para.7
borders but from the early 1970s drug enforcement agents developed Operation Springboard to seek the rendition of traffickers back to the United States. The policy was extended in the 1980s to terrorists also but, on 17 September 2001, a Presidential Finding gave the CIA virtual *carte blanche* to take whatever action it deemed necessary regarding individuals either suspected of involvement or of planning future attacks and the policy of ‘extraordinary rendition’ was put into place. The point being that the policy resulted directly from the application of the precautionary principle to counter-terrorism. There are many aspects of this issue that cannot be examined here but given that it is both illegal (‘extra-judicial’) and of dubious effectiveness what does it teach us about the prospects for intelligence oversight?

In comparison with the oversight of national state agencies, it is the very informality and enhanced secrecy of cross-national and -sectoral networks that attracts practitioners and inhibits oversight. For example, Dick Marty’s investigation for the Council of Europe found that, in developing extraordinary rendition:

In terms of protections, the US Government insisted on the most stringent levels of *physical security for its personnel*, as well as *secrecy and security of information* during the operations the CIA would carry out in other countries. And, according to our sources, the CIA determined that the bilateral arrangements for operation of its HVD programme had to *remain absolutely outside of the mechanisms of civilian oversight*. This is why the CIA selected military intelligence agencies in Poland and Romania rather than their usual civilian partners.

We can identify some areas of possible development in order to develop much needed oversight of intelligence networks within Europe and indeed beyond. Organizationally, national oversight should be functional, not institutional. Failing that, overseers must develop their own networks; if

---

58 Ibid., para. 79 (emphasis in original).
59 Ibid., para. 168, emphasis in original. It is estimated that over 100 people disappeared as part of the HVD programme.
60 A very useful collection of articles on this issue has just been published: Hans Born, Ian Leigh and Aidan Wills, *International Intelligence Cooperation and Accountability* (Abingdon: Routledge 2011).
there is more than one oversight body within the state, they should use 'statutory gateways' to enable them to cooperate on inquiries.\textsuperscript{61} Between states, some mechanisms are already in existence, for example, biennial International Intelligence Review Agency Conferences. These could be further developed in terms of sharing practice and information.

Also, there are some existing transnational bodies with potential in Europe, such as the European Parliament (EP) and Council of Europe (CoE) that have both examined extraordinary rendition. But while the advantage of such transnational bodies is that they transcend the national, they lack democratic legitimacy and have no authority over national governments to compel disclosure. This hindered Marty:

We must condemn the attitude of the many countries that did not deem it necessary to reply to the questionnaire we sent them through their national delegations. Similarly, NATO has never replied to our correspondence.\textsuperscript{62}

Although there are some supra-national European bodies with intelligence functions – Europol, Sitcen, Frontex – that have been established with some limited oversight mechanism, their contribution is minimal given that almost all significant intelligence sharing and cooperation occurs bi-laterally.

The law has a greater role now in governing intelligence than 25 years ago, but it ‘empowers’ as well as ‘limits’ agencies. Yet the development of rules by national and supranational bodies, their application and judicial oversight by, for example, the European Court of Human Rights (ECtHR) can make a contribution to the task of overseeing intelligence, especially regarding its propriety. It is also noteworthy that courts are now less deferential on security matters than even ten years ago – 23 Americans, mainly CIA officials, have been convicted in Italy for their part in the extraordinary rendition of Abu Omar in 2003 and face arrest if they travel to Europe. However, the courts in Germany have upheld the government’s decision not to seek the extradition of CIA agents allegedly involved in the rendition of Khaled el-Masri, despite the issue of an arrest warrant.\textsuperscript{63}

Although the informality of networks that is prized by practitioners reduces the impact of law, Richard Aldrich argues that the law has still had more impact in terms of intelligence oversight since 9/11 than ‘toothless’ political mechanisms.\textsuperscript{64} However, while the law might occasionally have impact

\textsuperscript{61}Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar, \textit{A New Review Mechanism for the RCMP’s National Security Activities} (Ottawa: Public Works and Services 2006).

\textsuperscript{62}Marty, \textit{Alleged Secret Detentions and Unlawful Inter-state Transfers}, 20.

\textsuperscript{63}Melissa Eddy, ‘Court Rejects el-Masri Suit against German Government’, \textit{The Miami Herald}, 10 December 2010.

through cases brought before the courts, the vast majority of intelligence operations never do come to court. The law is little use for regular auditing and monitoring.

Since a common feature of covert action is that intelligence agencies use ‘grey’ financial channels, agencies should be required to inform their oversight committees of financial incomings and outgoings with other agencies and the corporate sector in connection with operations, training, equipment, etc. Much intelligence sharing takes place electronically and there is potential for built-in auditing that can be accessed by overseers. For the foreseeable future, however, institutional forms of oversight of intelligence networks will remain largely undeveloped and, as we saw in the case of rendition, it is most likely to occur as a result of informal coalitions of parliamentarians, lawyers, researchers, journalists and those working in civil society organizations. All of these can contribute to ‘regulation through revelation’.65 Indeed, in an age of Wikileaks, Cryptome et al., we should make a virtue of necessity and encourage all the various forms of oversight as they emerge in both official and unofficial contexts.

Conclusion

The pressures on intelligence agencies to ‘deliver results’ and on parliamentary and other oversight bodies to relax oversight are greatest when security fears and uncertainties are at their height. This is the danger of the oft-quoted need to ‘balance’ security and rights; the need for oversight is actually greater at times such as this in order to promote effectiveness and prevent abuses of human rights. Furthermore, risk-shifting by means of intelligence cooperation must not become the mechanism for out-sourcing illegality.

To the extent that counter-terrorism is now based on the precautionary principle, the analysis of new policies and laws is required before – envisaging unintended outcomes – and after enactment to assess impact.66 Such policies can cause new risks and/or transfer risks to new populations and even if a risk is determined to be ‘real’, the countervailing costs of trying to remove or reduce it may still be judged to be excessive and unjustifiable. ‘(T)he analysis of risk-risk tradeoffs is . . . the sensible response to check excessive or narrow-minded exercise of government power.’67 If political executives are unwilling to do this, then parliaments and other overseers must.

In order to counter tendencies towards the ‘security’ state, overseers in the state sector must:

- remain sceptical of what they are told in the face of the demands of security and secrecy;
- develop a greater ‘cosmopolitan’ outlook, for example, the Belgian Standing Intelligence Review Committee has initiated a number of pan-European measures to improve oversight;
- build on existing transnational bodies, e.g. European Parliament, Council of Europe; and
- foster relationships with each other and wider interested community of researchers, journalists, and non-governmental organizations (NGOs).

But, intelligence now involves many actors beyond the state sector and careful attention must be paid to a broader ‘political economy’ of corporate intelligence and the counter terrorism industries. This has not been mapped outside of the United States and it may well be that ‘intelligence–industrial’ complexes are relatively under-developed elsewhere but technological developments and the needs of ‘protective security’ will require something similar in any liberal capitalist economy.

Are any of these issues ones that intelligence studies would not have been asking before the convergence with risk analysis? To the extent that most intelligence work remains centred on the consequences of malign intentions rather than broader safety concerns, then nothing has really changed. But what has changed is the perceived increase in the uncertainty of threats and the consequent pressure to act in a precautionary manner. It is this that has brought intelligence work into greater proximity with areas of risk analysis such as finance and climate change. As academics, our research, explanations and teaching must contribute to realistic analyses of complexity and uncertainty so they do not degenerate into ignorance and provoke security panics.

Acknowledgements

Earlier versions of this article were given at CAST/IARU Conference, 29–30 October 2009, Copenhagen, and the conference of the International Studies Association, Montreal, March 2011. I am grateful to participants at both of those for their comments. Special thanks to Stefan Brem, Mark Phythian, David Strachan-Morris and Michael Warner for their detailed comments on this article and to Stuart Farson for earlier exchanges on this issue that were very useful.