ABSTRACT The post-9/11 period and its emphasis on tackling terrorism has had a fundamental impact on the business of intelligence, not least in raising some very difficult ethical issues to the forefront of debate. Many of these issues are interwoven with the business of ‘policing globalisation’ in the modern era. The changes and developments offer new opportunities in Intelligence Studies for exploring ethics, and the role of the intelligence function within a modern liberal democracy. The questions posed by the new threat picture for such states offer something of an ‘intelligence dilemma’, which must balance the provision of good security with respecting civil liberties and ensuring the continued support of the population for security and intelligence policy. This article examines the intelligence dilemma within the framework of five dimensions: globalisation, risk and resilience; the question of a ‘surveillance society’; the ‘intermestic’ challenge in the new threat picture; difficulties around the use of covert action and cyber capabilities; and partnership risks. The article suggests that a deeper analysis of these issues represents opportunities for taking Intelligence Studies in new directions.

Defining the Intelligence Dilemma

Ten years on from the terrorist attacks in the US on 11 September 2001, some of the implications for how the intelligence business is, or should be, adapting to the evolving picture of this new threat are starting to become clearer. At the same time, some of the difficulties and challenges to the intelligence business posed by contemporary counter-terrorism are also, ominously, starting to emerge from the mist. In many ways, these challenges are causing a renewed focus on serious questions about how an intelligence capability in a modern liberal democracy should act, and where its boundaries should rightfully be. Intelligence-gathering has never been a straightforward business in terms of the ethical issues it raises for a liberal society. In some ways, the post-9/11 era in which counter-terrorism has taken on a newly elevated priority in the intelligence world does not mark an
entirely new beginning. Terrorism threats have been tackled in various shapes and forms for many years prior to 2001, and the 9/11 attacks themselves (despite the intelligence failings) did not come out of the blue entirely. In other ways, it could be argued that 9/11 did mark a sudden and critical watershed, not only in Western foreign policy and national security posture, but also in the development of intelligence tradecraft and capability.

Aldrich goes slightly further back in history to the fall of the Berlin Wall in 1989, noting that intelligence and globalization in the post-Cold War era have become increasingly intertwined.\(^1\) This has happened in a number of ways. Firstly, rising transnational threats such as international terrorism have deftly ‘ridden the wave of globalisation’.\(^2\) In turn, these threats call for different responses from those appropriate to traditional state-on-state conflicts that dominated national security thinking in earlier eras. Modern threats arising from globalization are harder to find and track, are more fluid, and are more embedded within civil society. Intelligence, increasingly, has become ‘a mode of policing the underside of globalisation’\(^3\).

A notion of ‘security dilemma’ was a construct that emerged right at the beginning of the Cold War, in the 1950s, with Herz and Butterfield.\(^4\) The logic was a Realist one (Mearsheimer described Herz as a pioneer of ‘offensive realism’),\(^5\) whereby states in an essentially anarchic system would naturally suspect one another of nefarious designs and would arm themselves accordingly. The theory seemed to work well for the politics of the Cold War and the arms race between East and West, but there was debate about what would happen at the end of the Cold War. Writing in the year that the Soviet Union finally collapsed, Booth suggested that the traditional notion of the security dilemma ‘will become a less pressing feature’ as the ‘institution of war will decline in utility’.\(^6\) For many, the 1990s proved to be a false dawn, however, as conflict and security crises continued around the world. As Ripsman and Paul noted of the post-Cold War era, ‘there is little evidence that globalization has transformed the pursuit of national security’, and ‘states still endeavor to protect themselves with traditional national military apparatuses’.\(^7\)

Placing together the issues of a continued need for traditional security responses despite the changing threat picture, with an enhanced significance

---

\(^2\)Ibid., p.28.
\(^3\)Ibid., p.29.
\(^5\)Ibid., p.494.
for intelligence in ‘policing the underside of globalisation’, I would argue
that a new ‘intelligence dilemma’ is emerging in the post-Cold War world
alongside the traditional notion of security dilemma. The intelligence
dilemma is subtly different, in that it takes account of a gradually increasing
public expectation of openness and accountability in the activities of the
intelligence agencies. This confronts, uneasily, the need to enhance and
develop intelligence capabilities in order to effectively tackle threats that are
perceived to be rising and growing more complex, such as those from
international terrorism and cyber-attack. The key word at the centre of the
new intelligence dilemma is ‘ethics’, and specifically how intelligence
agencies in liberal democracies can maintain their ethical code and values
in the face of enhancing their capabilities.

Much good research has been undertaken on ethics and intelligence after
the end of the Cold War. Some of this has looked generally at the ‘heart of
darkness’ of modern intelligence activities post-Cold War and post-9/11,\(^8\)
while other studies have focused on specific issues such as the pitfalls of
increased international intelligence cooperation in fighting terrorism.\(^9\) More
fundamental questions of intelligence and ethics in the contemporary era
have received attention from Quinlan, Herman, Gendron, Shelton and
Goldman, among others.\(^10\) Many of these have noted the assertion
supposedly once made by the CIA officer, Duane Clarridge, that ‘intelligence
ethics’ is essentially an oxymoron.\(^11\) In confronting this charge, Quinlan and
Gendron in particular have looked at whether theories of ethics in warfare,
and notably the notion of ‘just war’, can suitably be translated to the
business of espionage. Others, such as Marx,\(^12\) have looked at sectoral issues
such as the ethics of ‘new surveillance’ in the age of the Internet, or at the

\(^8\)See for example P. Gill, ‘Security Intelligence and Human Rights: Illuminating the “Heart of
Darkness”?’, *Intelligence and National Security* 24/1 (2009) pp.78–102; or L. Scott and R.G.
Hughes, ‘Intelligence in the Twenty-first Century: Change and Continuity or Crisis and
Transformation?’, *Intelligence and National Security* 24/1 (2009) pp.6–25; both of which
resulted from the third conference of the Centre for Intelligence and International Security
Studies (CISS), University of Aberystwyth, at the University of Wales Conference Centre in
Gregynog. See L. Scott, R.G. Hughes and M.S. Alexander, ‘Journeys in Twilight’, *Intelligence

\(^9\)See for example, Aldrich, ‘Global Intelligence’, p.29.

\(^10\)M. Quinlan, ‘Just Intelligence: Prolegomena to an Ethical Theory’, *Intelligence and National
Security* 22/1 (2007) pp.1–13; M. Herman, ‘Ethics and Intelligence after September
Just Intelligence: An Ethical Framework for Foreign Espionage’, *International Journal of
Intelligence and CounterIntelligence* 18/3 (2005) pp.398–434; A.M. Shelton, ‘Framing the
Oxymoron: A New Paradigm for Intelligence Ethics’, *Intelligence and National Security* 26/1
(2011) pp.23–45; J. Goldman (ed.), *The Ethics of Spying: A Reader for the Intelligence
Professional* (Lanham, MD: Scarecrow Press 2006).


more general question of political and security ethics in a period of international, indeed transnational, terrorism, as has Ignatieff.\textsuperscript{13}

Ethical approaches to intelligence have varied along a spectrum, with Realist approaches at one end (which consider it appropriate to protect the national interest in an anarchical world by whichever means are necessary), and Deontological approaches at the other (which consider that all forms of intelligence-gathering are fundamentally unethical).\textsuperscript{14} An example of the former would be the justification of the use of ‘waterboarding’ on terrorist suspects by the US authorities after 2001, while an example of the latter might be the suggestion by certain human rights groups that Western nations should cease all dealings with intelligence and security agencies in countries where terrorist and other detainees are frequently tortured. In the middle of the spectrum sits the Consequentialist approach, characterized by Herman’s ‘ethical balance sheet’,\textsuperscript{15} in which intelligence agencies make daily judgements on what it is proportionate and necessary to do to protect national security, while sticking as far as possible to high-level statements of ethical behaviour such as the European Convention on Human Rights (ECHR). There is much evidence that most Western intelligence agencies sit very much within the Consequentialist space at the time of writing.

Linked to question of ethics and intelligence is that of legality, and perennial questions of keeping within both the letter and the spirit of the law. In the UK, the notions of ‘proportionality and necessity’, which are part of the operational authorization process, are derived from the Human Rights Act, which allows the government to deviate from the right to the protection of privacy of the individual, on valid and appropriate national security grounds. Proportionality and necessity are not black-and-white concepts, however, but more a case of value-judgement depending on the circumstances. Omand suggests that ‘it is difficult to overstate the overall impact in recent years of . . . legislation on the ethos of the UK agencies in creating a disciplined culture within the agencies, while enabling them to carry out a full range of intelligence gathering operations for authorized purposes’.\textsuperscript{16} How far such a ‘disciplined culture’ has always acted in accordance with the law will be tested with the forthcoming Detainee Enquiry under Sir Peter Gibson, which will look at whether British intelligence agencies were complicit in torture when dealing with foreign partner agencies on the interviewing of terrorist suspects.

On the domestic UK front, Bamford looked at the effectiveness of British intelligence in fighting the terrorists associated with the Northern Ireland ‘Troubles’, concluding that it was largely successful from the point of view


\textsuperscript{15}Herman, ‘Ethics and Intelligence’, p.345.

of preventing attacks despite some concerns over specific aspects of the policy such as ‘stop and search’ and the targeting of specific ‘suspect communities’.\textsuperscript{17} Campbell and Connolly, meanwhile, have taken a more critical stance on this period, and particularly on the military-oriented phase of the Troubles, concluding that it was not a good model for contemporary ‘War on Terror’ thinking.\textsuperscript{18} In terms of the more recent terrorist threat from Al Qaeda-related groups and the ideology they inspire, Briggs has looked at the community-engagement model of intelligence-gathering and its pitfalls.\textsuperscript{19} Generally, analysis of the government’s ‘Preventing Violent Extremism’ (PVE) policy within the Counter-Terrorism Strategy (CONTEST) has tended to focus more on the problems of linking policing with community cohesion, than specifically on the problems posed by intelligence-gatherers themselves. On this relatively fresh issue there is some debate but a lack of in-depth research. Some, such as Maher and Frampton, have suggested that the Security Service (MI5) has confined itself unhelpfully to the ‘narrow’ target of terrorist attacks themselves rather than the broader question of ‘subversion’ by Islamist organizations.\textsuperscript{20} Kundnani takes a slightly different tack, arguing that the PVE agenda has widened intelligence-gathering in dangerous and sinister ways, by linking community and local authority bodies together with the police in a process of information and intelligence exchange on individuals in the community.\textsuperscript{21} This has led to the growth of a surveillance culture amongst bodies and processes that should be concerned with community support and development.\textsuperscript{22}

Placing all of these issues together, it seems clear that opportunities exist for a deeper research agenda within Intelligence Studies which confronts the newly emerging and perhaps unique ethical challenges to intelligence in the post-9/11 counter-terrorism era, and offers recommendations for how states and their intelligence sectors can best address the issues within a modern liberal democracy. These are issues of great contemporary relevance. As Scott and Hughes argue, ‘intelligence has never played so prominent a role in the public affairs of western societies as it does today’.\textsuperscript{23} In thinking about counter-terrorism policy more generally, Rosendorff and Sandler highlighted the ‘proactive response dilemma’ that faces liberal democracies, whereby too weak a response to a terrorist threat risks a loss of public confidence and

\textsuperscript{17}B.W.C. Bamford, ‘The Role and Effectiveness of Intelligence in Northern Ireland’, \textit{Intelligence and National Security} 20/4 (2005) p.603.
\textsuperscript{22}Ibid.
\textsuperscript{23}Scott and Hughes, ‘Intelligence’, p.6.
support for the government, while too strong a response risks undermining the values of a liberal democracy and alienating many in the population, not to mention encouraging support for the terrorists.\textsuperscript{24} I would argue that a subset of this process is an ‘intelligence dilemma’ for liberal democracies. This is characterized by the trade-offs inherent in balancing the need to provide strong security through surveillance and espionage, opportunities for which have expanded and developed in the age of globalization through the massive increase in availability of personal data and the means of collecting that data, with the need to ensure that ethical standards and the protection of human rights integral to the values of a liberal democracy are preserved. These are ethical questions for the intelligence-gatherers themselves as much as for the general public they serve.

I will look at this notion of intelligence dilemma in terms of four dimensions. First is the question of capitalizing on surveillance opportunities and developing new capabilities to do so, while avoiding charges of ‘Orwellianism’ and creating an intolerable surveillance state. The second dimension is closely related to the first, and involves the challenge of effectively working across blurring domestic and international boundaries engendered by globalization, and the way in which this process affects security threat and intelligence-gathering as much as it does many other sectors of society. The need in this area, particularly with respect to the contemporary terrorist threat, is to gather intelligence on individuals embedded deep within civil society at the local and regional levels, many of whom will be nationals of the state itself. Thirdly, much has been discussed over the years about the question of intelligence agencies and covert action. These debates are still relevant in the contemporary era, not least since 9/11 has seen a swing back towards covert operations and targeted assassinations of terrorist high-value targets (HVTs). Increasingly added to these activities, however, is the new component of active cyber operations, which are, as yet, little understood and little debated from an ethical point of view. Fourthly, and finally, the modern era of counter-terrorism throws up the dilemma of working with a wider range of international intelligence and security partners, while maintaining standards of human rights protection and avoiding charges of complicity in torture or degrading treatment of detainees. These four dimensions together comprise a critical agenda for further research in contemporary Intelligence Studies.

Globalization, Risk and Resilience

In discussing the manner in which globalization has affected the terrorist threat and responses to it, it is worth exploring briefly what exactly this process entails, so as to avoid Aldrich’s not unreasonable accusation that social scientists rarely pause to define the term.\textsuperscript{25} McGrew provides a useful


\textsuperscript{25}Aldrich, ‘Global Intelligence’, p.28.
conceptualization of globalization as ‘a fundamental shift or transformation in the spatial scale of human social organization that links distant communities and expands the reach of power relations across regions and continents’. Al Qaeda, for example, is essentially a stateless movement, which speaks to a religiously bound international community without reference to national borders and identities, and does so by using the Internet for social networking, recruitment, propagandizing and training. One of the ways in which this impacts the West is in the phenomenon of young radicalized foot soldiers for Al Qaeda travelling abroad with ease and relative anonymity to receive training in terrorist techniques, which they then bring back to the West. In some cases, radicalized recruits do not even need to travel abroad for their indoctrination and training, as they are able to access instruction remotely over the Internet, or through contact with other recruits or ideologues. The accelerating processes of globalization in such areas as international mobility, and information and communications technology, are essential elements of this process. We should recall that civilians who had freely entered the US to attack it from within conducted the 9/11 attacks, which killed more people than the Japanese attack on Pearl Harbor in 1941.

As the IRA noted in a message to the Thatcher government after the 1984 Brighton bombing, ‘remember we only have to be lucky once; you have to be lucky always’. The terrorists very often hold most of the cards when it comes to planning the next move. The government in turn can never completely protect itself and its citizens against a determined terrorist threat, and can never be absolutely sure it has complete penetration of the terrorist movement. So the calculation is one of risk management rather than absolute prevention. Minimizing the number of attacks and their severity may well be the best that can be done.

In protecting against an existential threat such as Soviet invasion or annihilation in nuclear conflict, a government could not aim for an 80 per cent solution: it would not be enough to only partially repel the attack. So the deterrent had to be complete. With terrorism, on the other hand, aside from the inherent impracticality of catching every single terrorist who is moving around freely within a democratic state (assuming you could find them), there is the added risk that an absolute security response would destroy the very fabric of society in a free and democratic state and make life

28Ibid.
intolerable. In a sense, the government would run the risk of doing the terrorists’ work for them.

As Sir David Omand, a strong advocate of the risk management approach to modern security, has noted, tackling threats such as terrorism in the future ‘is going to have to be guided by a security strategy that embodies these post-Cold War shifts in national security thinking towards focusing on the protection of the citizen, anticipation of risks and building enhanced societal resilience’.30

The element of anticipation here is complicated. In these cases, the sense is not that individual events can necessarily be predicted beforehand, but just that the overall pattern of threat is predictable. It is widely foreseen, for example, that a terrorist attack in the UK is quite likely at the time of writing, since there have been attempted and successful attacks in the recent past, and there is no reason to suspect that the motivation for such attacks has disappeared. The Terror Threat Level in the UK at the end of 2011 was set at ‘Substantial’, meaning that ‘a terrorist attack is a strong possibility’.31

The successful prediction of individual attacks, however, will be a sporadic process. Sometimes good (accurate) intelligence will allow this, but sometimes it will not, as the attacks of 7 July 2005 in London demonstrated. These attacks led to a number of investigations into the performance of the intelligence agencies, and particularly the Security Service (MI5). Of particular interest in the 2005 case was the discovery that two of the suicide bombers involved had been seen the year before in connection with another intelligence operation (Operation Crevice), but they had been assessed as being of peripheral importance and not developed further. The oversight body for the intelligence agencies in the UK, the Intelligence and Security Committee (ISC), reported in 2009 that the judgements made by MI5 at the time were ‘understandable and reasonable’,32 given the fragmented nature of the information available and the need to prioritize finite resources. The ISC report further stated that:

[W]e must be realistic. Despite the increased efforts of the Agencies, and the increased resources at their disposal, the odds are stacked against them . . . The attacks on 7 July 2005 . . . demonstrate that there will always be gaps in intelligence coverage. It is an uncomfortable truth that, at some time in the future, and without any prior warning, it is very possible that the UK will be the subject of another terrorist attack.33

33Ibid., p.55.
A 2011 inquest into the murders committed in the 2005 attacks, which was led by Lady Justice Hallett, also concluded that MI5 could not be held to be culpable for intelligence mistakes and failures around the attacks.\footnote{E. Addley, ‘7/7 Survivors End Battle for Public Enquiry into Bombings’, \textit{The Guardian}, 1 August 2011.} This has left the families of the victims unsatisfied as to whether justice has been done and whether the intelligence agencies have been properly held to account for their failings, although the families have now abandoned their long fight for a full public enquiry into the attacks.\footnote{Ibid.} In this episode we can see one of the key over-arching elements of modern intelligence dilemma in the contemporary counter-terrorism era. The nature of intelligence-gathering on modern transnational threats such as international terrorism is inherently diffuse and requires decisions to be made on finite resource prioritization. It is unrealistic to expect that MI5 and other agencies could have sufficient resources and capabilities to spot and disrupt every single potential terrorist attack (much as has always been the case to a large extent). This cannot be a process of complete threat mitigation, but rather one of limited risk management. Yet, how far the public understand this notion and are happy with it, particularly if they are unfortunate enough to have been directly affected by an attack, is a difficult question. Furthermore, how far the public will have confidence in the oversight process for behind-the-scenes intelligence activities, particularly where they suspect that mistakes and failures could be swept under the rug of secrecy, could be increasingly difficult and uncomfortable for the government. Gill notes that, while the ISC has perhaps exceeded expectations in its access to information, it could be accused of being too much a part of the management of the intelligence machinery rather than its overseer.\footnote{P. Gill, ‘Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the “War on Terror”’, \textit{Intelligence and National Security} 22/1 (2007) p.32.} This will continue to raise doubts about whether the ISC is the best vehicle for delivering intelligence accountability. The current chairman, Sir Malcolm Rifkind, has suggested that it should become a full parliamentary committee, reporting simultaneously to Parliament and to the Prime Minister, rather than directly to the latter as is currently the case.\footnote{‘Politicians Demand Extra Powers to Hold Spies to Account’, \textit{Daily Telegraph}, 13 July 2011.}

Rifkind also made the point that, in the 16 years since the ISC was established, ‘public expectation in terms of transparency and openness has increased significantly’.\footnote{Ibid.} More recently, the advent of Wikileaks has also posed some new questions about how far government should keep information secret, and how far they can continue to do so in the future. Page and Spence conclude that Wikileaks has demonstrated a feeling that diplomacy in the US and probably amongst its allies, has been ‘undoubtedly abusing its right to decide what is secret and what the public have a right to

\footnotesize{\begin{itemize}
    \item \footnote{E. Addley, ‘7/7 Survivors End Battle for Public Enquiry into Bombings’, \textit{The Guardian}, 1 August 2011.}
    \item \footnote{Ibid.}
    \item \footnote{P. Gill, ‘Evaluating Intelligence Oversight Committees: The UK Intelligence and Security Committee and the “War on Terror”’, \textit{Intelligence and National Security} 22/1 (2007) p.32.}
    \item \footnote{‘Politicians Demand Extra Powers to Hold Spies to Account’, \textit{Daily Telegraph}, 13 July 2011.}
    \item \footnote{Ibid.}
\end{itemize}}
know’. This has happened at a ‘time of diminished moral authority’, when ‘public scepticism is high’ following the debacle of the intelligence case for the war in Iraq and issues such as the MP expenses scandal. The phenomenon of Cosmopolitanism does not just mean the growth of a sense of global citizenship, but also, as Falk describes, a drive to extend transparency and accountability to all levels, including to the ‘undertakings of governments themselves’. Wikileaks has arguably fed into this gathering desire for the flashlight of accountability to be shone into every corner of the state’s activity. Such shifts and developments in public opinion will increasingly be critical features of the post-9/11 security and intelligence landscape and will shape the challenges that the contemporary intelligence sector will face, at least in liberal democracies.

Surveillance Society?

Writing at the end of the twentieth century, Gary Marx identified the opportunities for ‘new surveillance’ that were arising with the rapid development of communications and information technology. What makes the current form of surveillance new is its multi-faceted technological characteristics that go far deeper than mere information and intelligence-gathering. The expansion is not only in volumes of data, but also types (audio, visual, telemetric and even biochemical), within which the increase in availability of personal data is just ‘a tiny strand’ of the expansion of knowledge, and of ‘the centrality of information to the working of contemporary society’ in which everyone leaves a digital footprint. Added to this, advances in technical capabilities for databasing, data-mining and modelling information mean that surveillance now means a lot more than just gathering data and reading it. ‘We are becoming a transparent society of record’, writes Marx, such that ‘documentation of our history, current identity, location, physiological and psychological states, and behaviour is increasingly possible’.

With globalization, as President Kennedy used to say, ‘a rising tide floats all boats’, so transnational security threat actors such as terrorists are making good use of the benefits of the information revolution much as are intelligence agencies. This offers tremendous new opportunities for the agencies, but also tremendous risks. The 2009 edition of CONTEST noted that the rising use of Internet-based communications posed a technical

40 Ibid.
43 Ibid., p.171.
44 Ibid.
capability threat to Signals Intelligence (SIGINT), which was based on older methods of intercepting communications and related data. It mentioned this in the context of a technical development programme called the Intercept Modernisation Programme (IMP), reports of which had started to emerge in 2008. While the details of this programme were not disclosed, anxiety in some quarters over its remit caused some media channels to label the proposed system as GCHQ’s ‘Big Brother database’.

The former Home Secretary, Jacqui Smith, had recognized that ‘the balance between privacy and security is a delicate one’ and expressed an intention to strike ‘the right balance between maximising public protection and minimising intrusion into individuals’ private lives’. Some observers, however, felt that there had been a ‘tipping of the balance in favour of state power and away from the individual’. Whatever the consensus of opinion, GCHQ took the unprecedented step in May 2009 of issuing a press release in which it sought to allay the fears of the public and to deny that it was planning to comprehensively monitor everyone’s communications.

In its statement, GCHQ stressed both the ‘necessity and proportionality’ of all its operations – words relating to the Human Rights Act provisions around invasions of privacy – and the fact that all of its activities are ‘meticulously’ in accordance with ministerial approval. ‘GCHQ does not target anyone indiscriminately’, said the statement, and ‘does not spy at will’. That GCHQ, an agency that very rarely comments on any operational or technical matters publicly (and, indeed, was only placed formally on the statute books in 1994) should choose to issue such an emphatic statement about the justification for its activities and the scrupulously legal nature of them, betrays both a greatly heightened awareness of public anxiety over some of the aspects of the ‘new surveillance’, and a desire to be more open and communicative in its methods. However, whether such statements will become more frequent is unknown at the time of writing. Clearly GCHQ recognizes the very delicate balancing act that Jacqui Smith identified, between winning the public’s trust and support for its activities and not crossing any ethical red lines.

In 2006, the Information Commissioner in the UK, Richard Thomas, commenting on the results of a Parliamentary Home Affairs Committee debate into surveillance capabilities in Britain, claimed that we were ‘waking

---

47HM Government, Pursue, Prevent, Protect, Prepare, p.73.
50Ibid., p.1.
up to a surveillance society that is already all around us’. He further noted that:

Surveillance activities can be well-intentioned and bring benefits. They may be necessary or desirable – for example to fight terrorism and serious crime, to improve entitlement and access to public and private services, and to improve healthcare. But unseen, uncontrolled or excessive surveillance can foster a climate of suspicion and undermine trust.

Recent research by Newcastle University identified a dichotomy in public perception between a need for privacy and the need to be protected from the anonymity of others. Eijkman and Weggemans, meanwhile, examined the rise of visual surveillance, taking the UK and the Netherlands as case studies. They noted the delicate balance between a likely growing public support for the extension of visual surveillance in the face of the domestic terrorist threat, while at the same time a risk of ‘excessive or arbitrary’ use of visual surveillance by ‘the authorities’, which could lead to fears in the public of the growth of a panoptic surveillance society. It is probably fair to say that the public would equate the intelligence agencies with the ‘authorities’ in this case, even if the agencies were not making as much use of visual surveillance capabilities themselves as were other departments such as the police. The important point concerns public perception of these issues and the need to maintain public trust that such capabilities are being used appropriately and proportionately.

The ‘Intermestic’ Challenge

The second dimension of the intelligence dilemma links to the first, and concerns the targets of new surveillance techniques. As Cha has observed, globalization has seen a blurring of traditional divisions between external and domestic security issues, some of which are now described rather inelegantly as ‘intermestic’ security threats. Organized crime, weapons proliferation and terrorism are all classic examples, and they increasingly require state intelligence agencies to work together with policing bodies and

---

other potentially uneasy bedfellows. In overseas contexts, this means militaries and intelligence agencies must increasingly work with state police bodies in gathering intelligence on terrorist adversaries: a process which is not without its logistical and ethical complications. At home, the July 2005 terrorist attacks in London raised the new realization that ‘home-grown’ terrorists using suicide-bombing were a threat on the British mainland, as much as individuals travelling into the country from outside.

The strand within CONTEST that has particular relevance to the linkage between terrorists in the domestic and international spheres is the Prevent strand, which aims to identify and tackle the radicalization process within local communities. This has proved to be one of the most complicated and controversial elements of the counter-terrorism response in the UK in the post-9/11 period. One of the many problems with Prevent in its early years was that many within the domestic Muslim community saw it as a thinly veiled front for spying on the community. The accusations were that, by coupling community cohesion projects and activities with a counter-terrorism agenda, the thrust of such work in the community inevitably felt like it was an underhand way for the authorities to gather data on the community for intelligence purposes. The police were placed in a particularly difficult position in this respect, since they were tasked simultaneously both with liaising with the local community and sitting on ‘intervention’ panels; as well as gathering intelligence on potential counter-terrorism cases and liaising with MI5 in so doing (through their local Special Branch units). As many in the British Muslim community will say, as taxpayers Muslims are no less keen than any other citizen for MI5 and the other intelligence agencies to fulfil their role in catching terrorists and keeping us safe. But they expect this to be an unseen business, and not for it to be undertaken covertly through community projects.

In many ways these issues remain a classic dilemma of intelligence-gathering on a subject such as terrorism within a modern liberal democracy, where the distinction between domestic and overseas individuals and activities is distinctly blurred. The people and authorities who will spot where particular problems are appearing deep within a community are either members of that community itself (to which end, good relations with the police are vitally important), or members of local authorities and statutory bodies working closely with the community, such as teachers, health workers, probation officers or council officials. How can potential intelligence leads from these quarters be channelled up through the system to the likes of MI5, without the whole process looking and feeling somewhat uncomfortable? Community expectations that MI5 work silently behind the scenes to establish their leads may, in fact, be an unrealistic expectation in

---

58Aldrich, ‘Global Intelligence’, p.28.
59In some areas, police constabularies established dedicated new police staff posts for the purpose called Prevent Engagement Officers (PEOs).
60Interviews with various local Muslim community representatives, southern England, May/June 2010.
the modern era. Yet, nobody wants to see a Stalinist situation where neighbour informs on neighbour for the wrong purposes, or where the police start to look like a repressive secret police. Writing just before the new government published the Prevent policy review, Thomas’s verdict on the programme was fairly damning, and suggested that the policy had left Britain in a ‘worrying impasse’ in terms of community relations.61

A difficult question for MI5 has been whether the current domestic terrorist threat in the UK is principally a threat of terrorist attacks, or is more than this in that it also comprises a subversive ideological component.62 As Maher and Frampton observed, the previous Labour government – and MI5 – were keen to say that there was not a threat of ‘non-violent subversion’ associated with the current terrorist threat.63 By this they meant that there was not an organized connection between Islamist groups that may seem to be ‘extreme’ in their rhetoric, and the terrorists connected with Al Qaeda’s ideology. Part of the rationale for this view was that the government could use members of the Muslim community who may be ‘close to the coalface’ of violent extremism to liaise with relevant vulnerable individuals and mitigate threats, but it may also have been through a fear of political risk in being seen to connect Islamic religious ideology with terrorism (and thus falling foul of ‘Islamophobia’).64 Nevertheless, for MI5, the question of whether ‘extreme’ ideological groups such as Hizb-ut Tahrir should be investigated in the same way that suspected elements of the Comintern were during the Cold War remains partially on the table. Again, there is something of a dilemma here for the intelligence-gatherers: to widen the front to include subversion entails considerable resource implications, not to mention political risk; but not to do so risks accusations of political correctness and complacency (even if the assessment is that such a linkage does not exist). Such issues are part-and-parcel of the current ‘intermestic’ terrorist threat, and the question of response strategies in a liberal democracy.

Covert Action, and Cyber Security

In history, covert action capabilities exercised by intelligence agencies have generated a great deal of debate, notably in the US in the 1970s with respect to the FBI’s anti-communist Counter Intelligence Programme (COINTEL-PRO), and the actions of the CIA in removing pro-Communist leaders in

---

62The Security Service Act of 1989 defines subversion as actions ‘intended to overthrow or undermine parliamentary democracy by political, industrial or violent means’, although MI5’s website makes clear that this was a relic of the Cold War and that ‘we do not currently investigate subversion’ <https://www.mi5.gov.uk/output/subversion.html> (accessed 4 December 2011).
63Maher and Frampton, *Choosing our Friends Wisely*, p.5.
64Ibid.
Latin American and elsewhere. As Michael Herman famously observed, ethical debates about intelligence may be moot as ‘no-one gets hurt by it, at least not directly’. This is true of passive intelligence-gathering, but, as Herman recognized, covert action raises a set of different questions, since people may well be hurt by it. In the post-9/11 era, secret renditions of detainees to third countries where they may be tortured, and targeted assassinations of terrorist HVTs, often using Unmanned Aerial Vehicles (UAVs) or ‘drones’ which can cause collateral civilian casualties, have brought debates about the ethics of covert action back onto the table, particularly in such countries as Pakistan.

One area of capability that has, as yet, received little attention, is the question of active cyber activities by Western intelligence agencies and militaries. Very little is known about this yet, either in terms of the nature of the capability or whether and how it has been used offensively. Referring to the work of the Cyber Security Operations Centre (CSOC), which is based at GCHQ in Cheltenham, the former Minister for Cyber Security, Lord West, mentioned that ‘it would be silly to say that we don’t have any offensive capability from Cheltenham, and I don’t think I should say any more than that’. It is clear that cyber-intelligence and cyber-security are very much both poacher and gamekeeper activities. Most advanced nations now have cyber capabilities within their defence departments. The leviathan in this area is the Pentagon-based Cyber Command (CYBERCOM) in the US, which commenced operations in 2010. CYBERCOM specifies that it conducts both the ‘defense of specific Department of Defense information networks’, and ‘full-spectrum military cyberspace operations’. In the UK, the Minister for the Armed Forces, Nick Harvey, outlined the logic of this approach, noting that ‘action in cyberspace will form part of the future battlefield, but it will be integrated rather than separate, complementary rather than alternative’.

This area of capability should reasonably be subject to ethical debate, since it is effectively a new form of covert action. It may be that the ‘effects’ of offensive cyber-activities will always be hard to determine, as much as cyber-attacks are difficult to pinpoint and to define, but there will undoubtedly be situations in which harm will befall some individuals as the result of hostile cyber-activities. Furthermore, if the Internet is supposed to be a bastion of free information and debate, what are the ethical considerations, if any, of manipulating and perverting it for intelligence or military purposes? If we...

---

66Herman, ‘Ethics and Intelligence’, p.342.
criticize states such as China for limiting or manipulating public access to information on the Internet, where do the West’s ethical boundaries lie on this topic? Such questions are unanswered or even possibly unasked at present, but could usefully be subject to future debate.

Partnership Risks

In July 2010, the Prime Minister announced that an independent enquiry (the ‘Detainee Enquiry’) was to be undertaken by Sir Peter Gibson. The remit of this enquiry was to ‘look at whether Britain was implicated in the improper treatment of detainees, held by other countries, that may have occurred in the aftermath of 9/11’. The need for such an enquiry has been prompted by a number of cases since 2001. The most significant of these for the UK has been that of Binyam Mohamed, who, after being picked up in Pakistan in 2002, spent seven years in custody, with the remaining four in Guantanamo Bay. Mohamed claims that, in the first two years of his detention, he was moved between Pakistan, Morocco and Afghanistan, where the authorities periodically tortured him. He claims that British intelligence officials interviewed him during this period and must have known he was being ill-treated, but turned a blind eye. In November 2010, Mohamed and six others with similar cases, who became collectively known as the Guantanamo Seven, agreed to drop their cases against the British government in return for substantial out-of-court settlements totalling several million pounds.

Similar cases have afflicted other partners in the post-9/11 era. Aldrich outlines the case of the Canadian citizen Maher Arar, who was rendered by the US to Syria via Jordan, where he was tortured. The O’Connor Commission in Canada eventually cleared Arar of all terrorist charges and awarded him over C$10 million in compensation. The implications of such cases for intelligence agencies and their governments are twofold. Firstly, partnership with the US in the post-9/11 era has exposed some Western agencies to severe reputational strain, where they have been seen to be complicit in robust covert activities such as the extraordinary rendition of terrorist detainees to third countries, or indeed to Guantanamo Bay. Secondly, direct relationships with third countries such as Syria, Jordan, Pakistan, Afghanistan and numerous others, whose record on human rights leaves very much to be desired, often means that intelligence dividends

---


71 Prime Minister David Cameron, statement in House of Commons, 6 July 2010. Cited in ‘The Detainee Enquiry’ (<http://www.detaineeinquiry.org.uk/?gclid=CM_mkPq89KsCFQUNdXodXsdnKg>).


73 Ibid.

gained from such relationships need to be balanced with potentially severe reputational risk and accusation of undermining the very values that liberal democracies supposedly hold dear.

At the diplomatic level, the somewhat unsatisfactory instrument that has been used to tackle this problem has been that of ‘diplomatic assurances’ sought from certain countries, whereby pledges are made that human rights in dealing with shared detainees will be upheld. In the case of Afghanistan, this process has been represented by an exchange of letters undertaken in 2007 between a coalition of the US, Canada, the UK, the Netherlands, Norway and Denmark, and the Afghan government on the question of detainee transfers.\(^7^5\) The letters provide for officials to have access to Afghan detention facilities, to interview transferees in private if required, and for the same privileges to be accorded to the International Committee of the Red Cross, UN Human Rights bodies and the Afghan Independent Human Rights Commission (AIHRC). The Afghan government pledged that its intelligence and security agency, the National Directorate of Security (NDS) would issue instructions to all regional offices informing them of these agreed procedures.\(^7^6\) It was a breakdown in this agreement with regard to the UK in early 2009 that led to the UK military to join the Canadians in placing a freeze on all transfers of detainees to the NDS until further notice.

Meanwhile, in the UK, 2010 saw the initiation of a case for judicial review of Britain’s detainee transfer policy in Afghanistan, brought by a prominent peace activist, Maya Evans. The case centres around nine specific instances of transfer, mostly in 2009 and mostly involving the NDS’s Department 17 facility in Kabul. The allegations suggest that the detainees were subjected variously to ‘beatings, sleep deprivation, stress positions, electrocution, and whipping with rubber cables’.\(^7^7\) Michael Fordham QC accused the British government of relying on ‘manifestly unsafe’ diplomatic assurances that detainees would not be mistreated, when the evidence was that NDS-led torture and abuse of prisoners was ‘endemic . . . even at a very high level’.\(^7^8\) The logical conclusion drawn by this and a number of other reports by organizations such as Human Rights Watch (HRW) is that the practice of handing over detainees to the Afghan authorities should cease immediately until proper assurances can be obtained that human rights will be respected.\(^7^9\)

\(^7^6\) Ibid., p.7.
\(^7^8\) Ibid.
In many ways, this situation in Afghanistan highlights the extraordinary dilemma faced by intelligence agencies in the post-9/11 era. To not have any intelligence connections or dealings with the likes of the NDS in Afghanistan or the ISI in Pakistan, as the above reports have demanded, could expose Western national security to considerable risk. An essentially Machiavellian reading of the situation would suggest that, for those charged with ensuring our security in the face of serious transnational threats, complete withdrawal and isolation are not realistic – or even necessarily moral – options. Even a deontological notion of security, while recognizing that most intelligence-gathering is fundamentally unethical, can allow for some intelligence activities as a moral duty and imperative to protect a state.\(^{80}\) The situation may in fact call for the more consequentialist approach of Herman’s ‘ethical balance sheet’.\(^ {81} \) Perhaps, as Reveron noted, the current counter-terrorism strategy ‘requires cooperation of all interested states, no matter how distasteful they may be’. The challenge is therefore ‘to extract useful information from these foreign intelligence services without becoming tainted by their tactics’.\(^ {82} \)

**Conclusion**

Writing shortly after the 9/11 terrorist attacks in the US, Ignatieff suggested that the antithetical conception of human rights being good versus terrorism being inextricably bad, is not as simple as that: human rights is a ‘moral system’ with strengths and weaknesses, and for those fighting terror, human rights impose ‘limitations’ on counter-terrorism action.\(^ {83} \) This is, of course, extraordinarily fraught ethical territory. Terrorism and counter-terrorism have always provoked debate about whether there are cases in which the norms of human rights protection in a liberal democracy can sometimes be adjusted to suit the gravity of the situation. With the 9/11 attacks, such debates have taken on a greater intensity, as exceptionalist counter-terror policies have taken centre-stage in response to a threat which has been articulated as greater and more egregious than any faced before. As Tony Blair described it in giving evidence to the Chilcot Enquiry, 9/11 meant that the ‘whole calculus of risk’ had changed, and this meant that the responses had to change too. We have, he said, ‘a completely new security environment today’.\(^ {84} \) He was talking not only about the wider ambitions of the ‘new terrorist’ threat that the 9/11 attacks heralded, but also the prospect of

---


\(^{81}\) Herman, ‘Ethics and Intelligence’, p.345.


terrorists using unconventional weaponry such as chemical, biological, radiological or nuclear (CBRN) capabilities.

Huysmans describes the complications here as inherently political ones in terms of how exceptionalist security policies are justified and articulated.\textsuperscript{85} For a liberal democracy, this leads to a ‘paradox’ whereby ‘security knowledge and technology that is meant to protect liberal democracy against violence seriously risks to undermine it.’\textsuperscript{86} I have argued in this article that a subset of this paradox, which deserves much further attention, is an ‘intelligence dilemma’ within the context of contemporary counter-terrorism. This dilemma is multi-faceted, arising from the nature of the modern terrorist threat and the risk management approach it demands, and the actions of the intelligence agencies in appropriately and proportionately responding to it.

On the first point, the Director-General of MI5, Jonathan Evans, noted in a 2007 statement: ‘it is fairly unusual for the head of MI5 to speak at a media-focused event. But the issue of trust is highly relevant to the world of intelligence. All the more so as we tackle the most immediate and acute peacetime threat in the 98-year history of my Service’\textsuperscript{87} Evans was reflecting the manner in which, not only has the threat picture, and the subsequent size and nature of the security response in the post-9/11 era changed, but so has the public’s expectation of information about what the intelligence services are doing, and its expectation of assurances that the agencies are being held accountable for their action. Evans’s statement was followed in 2010 by the first ever statement by a serving head of SIS (MI6), Sir John Sawers.\textsuperscript{88} In his statement, reflecting on the difficulties of dealing with partners in counter-terrorism who do not hold good records on human rights, Sawers noted: ‘these are not abstract questions. They are real, constant, operational dilemmas. Sometimes there is no clear way forward’.\textsuperscript{89} We can sense here that the agencies are very much in a Consequentialist position on the ethical spectrum.

The heads of the agencies (including GCHQ with its press statement in 2009) have therefore acknowledged that the post-9/11 era poses particular issues of complexity, if not dilemma, in their intelligence operations, which intensify the questions around the proper limits of intelligence in a modern liberal democracy. Issues of surveillance and society, particularly within a technologically more complex environment, and one in which international and domestic boundaries are increasingly blurred, combine with more traditional preoccupations about covert action and dealing with partners

\textsuperscript{86}Ibid., p.322.
\textsuperscript{88}K. Sengupta, ‘MI6 Chief Admits to his “Dilemma” over Torture’, \textit{The Independent}, 29 October 2010.
\textsuperscript{89}Ibid.
whose records on human rights pose severe reputational risks, to create a deep and wide intelligence dilemma. The various elements of this dilemma will rightfully set the agenda for much further research and debate in Intelligence Studies.

Notes on Contributor

Dr Julian Richards is Co-director of the Centre for Security and Intelligence Studies at the University of Buckingham (BUCSIS). Prior to setting up BUCSIS, he spent 17 years working in intelligence and security for the UK government.