Intelligence and Counter Terrorism

Julian Richards, University of Buckingham

Introduction

Over the centuries, a number of key military strategists have stressed the central importance of intelligence to success in conflict. The sixth century BC Chinese strategist, Sun Tzu, is purported to have said that "foreknowledge" is what distinguishes successful generals and ensures their victories in conflict (Sun Tzu, trans. Griffith, 1963: 144). Similarly, the Prussian military strategist, Baron Karl Von Clausewitz, spent a great deal of time considering intelligence in his classic *On War*, noting that good judgement in interpretation of intelligence was absolutely essential for ensuring success (von Clausewitz, 1982). In these ways, intelligence can be seen as a critical tool of power for states in conventional conflict scenarios. Since the end of the Cold War which defined security through the second half of the twentieth century, many states have shifted a large portion of their national security discourse towards international terrorism rather than threats from other state actors. The controversially named War on Terror has been, in the view of many, the wrong way to conceptualise the struggle against transnational non-state terrorist actors (Howard, 2002). This might seem like a semantic argument of little import, but it is relevant when we consider the emergency powers that states contract to themselves when they officially declare a major terrorist threat. Many of these powers are to do with intelligence gathering capabilities.

In this sense, a critical discourse analysis of terrorism could suggest the phenomenon is a complex and sometimes Machiavellian element of power, whether it is exercised by the state or by a sub-state competitor. This is perhaps not the place to rehearse the very extensive debates around definitions of the "evanescent" notion of terrorism (Rapin, 2011), but merely to consider how states justify their levels of intelligence gathering capabilities in the face of supposed terrorist threats. At the conceptual level, consider, for example, how the Syrian Arab News Agency (SANA), the official news agency of President Assad, describes all of the forces against which he is fighting as "terrorists", rather than the complex rainbow of insurgents, terrorists and freedom fighters described in Western media. Motivations here are both to emphasise Westphalian duties in protecting the sovereignty and territorial integrity of the state, but also to attract international sympathy to the cause, since Western nations in particular can hardly disagree with the need to battle terrorists. In such a state of emergency, the state can make a claim to use the widest range of military and intelligence capabilities.

The interaction between terrorist and state actors has often been analysed using Game Theory approaches, since these allow for a notion of the critical interdependence between each side of the equation (Arce and Sandler, 2005). In this way, the gathering of intelligence by a state on a terrorist group can be seen as a legitimate and effective element of proactive and pre-emptive counter terrorism policy: essentially the “foreknowledge” of which Sun Tzu spoke. Similarly, terrorists will always be aiming to outwit the state, and they themselves will need information about the capabilities of counter terrorist policies and agencies in order to do so.

All of this leads to a complex contemporary debate in Western liberal democratic states in particular, whereby the expansion of intelligence capabilities runs up against civil liberties lobbies, who sometimes recall memories of totalitarian states such as communist East Germany in opposing their government’s supposedly oppressive designs. In response, the spectre of terrorism is often invoked to provide moral justification for enhanced intelligence gathering capability. Thus we can see an inextricable link between an appropriately articulated terrorist threat, and the intelligence component of counter terrorism policy.

Definitions of intelligence

Much as Terrorism Studies has undergone a long and laborious debate about how to define terrorism, so Intelligence Studies has had its fair share of definitional dialogue. The question of “what is intelligence” is one that has vexed and exercised many analysts. As Laqueur noted, intelligence can be seen both in terms of the agencies doing it, and the information they are gathering (Laqueur, 1985: 12). Much of the discussion centres around the differences between information and intelligence, with the latter viewed as some sort of refined or developed form of the former. In focusing on the nature of the information itself, many see secrecy as being a defining feature, not necessarily in the official governmental definition of being Secret, but in the sense that intelligence is generally information that an opponent or foe does not want you to see or to know. The father of structured intelligence analysis at the CIA, Sherman Kent, described this essential feature of intelligence as an inherent “clandestinity” (Shulsky and Schmitt, 2002: 172).

However, other theories look more at the potential utility of the information, that is, the fact that intelligence is a form of information that is actually useful for planning or strategizing in some shape or form (Sims, 1995: 4). This approach has the double benefit of giving an indication of the quality of potential intelligence (some of it is just data, which might look good but be of little benefit for policy-makers); and of widening our conception of intelligence usefully beyond traditional national security arenas and into the world of business, sport, and any number of other disciplines.

In the realm of counter terrorism, additional factors are important. Firstly, there is the question of intelligence tradecraft. In very broad terms, traditional clandestine intelligence gathering falls into two categories of activity. The first is human intelligence (Humint), which is famously one of the oldest human activities in history. This involves human beings gaining intelligence about their adversaries, either through persuading individuals to pass on sensitive information from inside a target group, or going undercover and penetrating a group. The second category of intelligence tradecraft can be loosely gathered under the umbrella of technical intelligence gathering (Techint). This entails gathering intelligence using technical means, such as the interception of electronic communications or other signals (Sigint), or the gathering of imagery data from satellites or other covert platforms (Imint).

Cutting across these activities is the business of clandestine surveillance. Traditionally this has been undertaken using human beings covertly following or observing targets, but increasingly, electronic means of surveilling targets are coming into the picture. These include geolocating targets through their satellite phones or other electronic devices, tracking vehicles using number-plate recognition cameras (ANPR), using CCTV, and a growing range of other capabilities.

Numerous other “ints” are sometimes mentioned in the realm of intelligence, such as open-source intelligence (Osint), which entails gaining intelligence from openly available documentation or sources, such as documents on the internet or listening to radio broadcasts; financial intelligence (Finint) and several others.

All of these forms of tradecraft are essentially about the methods of gathering intelligence and its sources, but returning to the end-to-end process of intelligence, one of the key debates in the field of particular pertinence to counter terrorism is the question of the connection between intelligence and action taken on the ground. This is the debate about covert action, which is as much an ethical debate as one about business process.

The traditional British model is that state intelligence agencies gather the intelligence but have no executive arm: whether and how the intelligence is acted upon is the realm of other agencies who receive that intelligence, such as the military or police. This allowed Herman to ponder whether the ethical debate about intelligence was pertinent at all, since “no-one gets hurt by it, at least not directly” (Herman, 2004: 342). In many other countries, however, intelligence agencies do have executive arms and will often act on their information. Classic examples include the CIA, who can use drones to fire missiles at terrorist targets on the basis of their own tactical intelligence, or indeed, in the past, engage in political assassinations. Similarly, Israel’s MOSSAD agency has an avowed policy of assassinating senior members of terrorist organisations such as Hamas or Hezbollah if the right intelligence comes their way. The ethical questions are not just about whether a state should use extreme violence to protect its national security, but also about the risks of the intelligence being wrong in such scenarios. On this point, the British or American systems are not necessarily any better than the other and both can be prone to fatal errors. The shooting dead by the police of a Brazilian citizen, Jean Charles de Menezes, in London in July 2005 when he was mistakenly identified as a fugitive terrorist is a case in point. Similarly, extreme scrutiny has been levelled at the time of writing towards the assassination in Syria of two British citizens by an RAF drone strike on the basis of intelligence that they were close to undertaking terrorist attacks on British interests. It is not clear what the outcome of such investigations will be, but any rate, the incident clearly challenges Herman’s point above about the limited effects of intelligence.

It should also be noted that, particularly in the post-9/11 era of terrorism and counter terrorism, not all significant intelligence on terrorism is gathered by state intelligence agencies. There has been an increasing emphasis in this period on “community intelligence”, since the targets of interest for the state have moved into domestic religious and ethnic communities that are potentially harder to reach, and are traditionally less engaged with the state authorities. Thus, police services in many countries have invested resource into community engagement activities, whether these are Homeland Security sub-stations in policing districts in the US, as Thacher’s fascinating account of Dearborn, Michigan describes (Thacher, 2005), or Prevent Engagement Officers (PEOs) in the UK, and numerous other models. Such activities in large part reflect the strategic policy shift in the post 9/11 era in counter terrorism, towards a greater element of pre-emptive and preventative action rather than solely on pursuit and interdiction activities. In the UK, this strand of activity is spearheaded by the Prevent strand of the Counter Terrorism Strategy (CONTEST), and is mirrored in the EU’s overarching strategy, launched under the UK’s presidency in the second half of 2005. For all its logic, however, preventative strands of counter terrorism policy have come to encapsulate many dilemmas for the state which are central to contemporary questions about the role of intelligence in this area of policy.

A brief history

For much of the twentieth century, state intelligence capabilities against defined national security threats were seen in a somewhat realist way, coloured in large part by the supposedly existential requirements of the Cold War, in which espionage and counter-espionage played large and highly significant roles. For many countries, traditionally defined security in the shape of military threats was the dominant priority, until the latter part of the twentieth century when a broadening of notions of security began to take shape (Sheehan, 2010; Buzan, Waever and de Wilde, 1998). This led in turn to a notion of "human security", which encapsulated a much wider range of security concerns than had previously been the norm (Fukuda-Parr, 2003). The collapse of the Soviet Union in 1991 and sudden end to the Cold War only served to accelerate a major reappraisal of security threat and response.

For intelligence capability within the liberal democratic state, thdeardenis conceptual shift in the latter part of the twentieth century led to a greater awareness of the need for accountability in what had previously been seen as an essential, if somewhat ugly tool of national security policy. In the UK, for example, 1989 saw the passing of the Security Service Act, which openly avowed the Security Service (MI5) and placed it and its authorised activities on the statute books for the first time. This was closely followed by the Intelligence Services Act of 1994, in which the Secret Intelligence Service (MI6) and Government Communications Headquarters (GCHQ) were similarly placed on the statute books, and a parliamentary oversight committee, the Intelligence Services Commmittee (ISC) and associated process were put in place. (The US has had a Senate Select Committee on Intelligence for much longer – since 1976 – in part due to its history of apparent misuses of intelligence during the 1960s and 70s.)

For parts of Europe, the Cold War period was also a time in which violent secessionist terrorist movements were active, such as ETA in Spain and the IRA in the UK, and revolutionary Marxist movements such as the Red Brigades in Italy and the RAF in West Germany. Some of these groups, notably Baader and Meinhof's RAF, had flirtations with the Palestinian terrorist movement which grew to become an international security concern in the 1970s.

The UK's long struggle with the Provisional IRA (PIRA) effectively came to an end in 1998, when the Good Friday Agreement was signed and militant groups including PIRA agreed to lay down their arms in favour of the workings of the devolved National Assembly of Northern Ireland. (Subsequent history shows that breakaway Irish Republican factions could continue to pose a terrorist threat, albeit on a smaller scale.) Assessments of the period of the Troubles, as they became known, which began in 1969 with the deployment of the British Army to Northern Ireland to quell inter-community sectarian violence, are that intelligence played an absolutely critical role in the disruption and eventual collapse of the PIRA's activities (Kirk-Smith and Dingley, 2009; Bamford, 2005). Within this picture, Jeffery suggests that Humint from inside of a terrorist organisation is the best intelligence a state can obtain (Jeffery, 1987).

The experience of this period seems to be that Humint in particular had a double effect on the PIRA organisation of anticipating attacks and plans and thus being able to avoid or counter them; while also tying-up the organisation's leadership with a continual paranoid investigation into who might be working for the enemy. For an organisation such as PIRA, this was not just administratively inconvenient, but also meant the physical loss of many of its operatives, since the penalty for being suspected of being a spy for the British was severe beating at best, and more often murder.

For the state, meanwhile, the brutal logic of using intelligence in this way had a further benefit of avoiding the costly and complicated process of having to bring people to trial, and having to consider whether and how sensitive intelligence could be used evidentially in court. As Robertson suggested, someone going to trial could actually have been considered a failure for intelligence, since it was much better to use it for further disruption and penetration of the target organisation (Robertson, 1987).

A modern corollary of this concept might the manner in which intelligence could be used to physically neutralise terrorist suspects in the field through drone strikes or other attacks. Such assassinations, happening as they tend to do in a context of "war" rather than a civilian context also avoid the need for a judicial process of the victims. Whatever the utility of such actions, however, experience suggests that states can suffer from this policy through challenges to their commitment to human rights and proper judicial processes.

Britain faced similar complications during its struggle with PIRA on two fronts. The first concerned interrogation techniques of terrorist suspects used by the British army, which the European Court of Human Rights ruled amounted to torture in 1976 (although this judgement was later overturned on appeal). The second involved accusations of an unspoken "shoot to kill" policy by counter terrorist forces. Various cases inflamed the latter debate, including the shooting dead of eight PIRA suspects in Loughall in 1987, and of three further PIRA members a year later in Gibraltar, in both cases by Special Air Service (SAS) soldiers. In each case, the state claimed that intelligence (which, in the Gibraltar case included that obtained through liaison with the Spanish authorities) indicated a real likelihood of a major terrorist attack, and that pre-emptive action was appropriate on grounds of national security and self-defence. This is exactly the same argument used by the state to justify the September 2015 drone attacks which killed Reyaad Khan and Ruhul Amin in Syria. Here we can see the point that intelligence, if assessed correctly, can allow a state to take exceptionalist action on the grounds of national security, similar to actions undertaken under the Laws of Armed Conflict. Many would welcome the protection of national security and likely avoidance of wider deaths so delivered, but the state also has to battle critics in these scenarios who will claim both that fundamental principles of human rights are compromised, and that intelligence cannot be scrutinised as to its veracity and utility since it always remains secret. As discussed below, this is one of the many dilemmas with which the liberal democratic state finds itself confronted on the boundaries between intelligence and counter terrorism.

More contemporary history shows that the hoped-for peace dividend of the post-Cold War period was punctured by the 9/11 terrorist attacks in the US in September 2011, which ushered-in a new period of conflict and counter terrorism policy. In the US in particular, the intelligence sector suffered a wave of criticism in the wake of the 2011 attacks for demonstrably having failed to anticipate the nature and extent of a new wave of terror. Comparisons were made with the Pearl Harbor attack during the Second World War, when a fatal lack of imagination about what the adversary might do proved pivotal (National Commission on Terrorist Attacks Upon the United States, 2004). Furthermore, the fact that such a low-cost and relatively primitive attack could be wrought on a nation that had spent billions of dollars on intelligence seemed all the more perplexing.

A more detailed analysis of the intelligence failure of 9/11 and its implications shows that the problems were multi-faceted. As the British and many others had discovered with earlier terrorist problems, terrorism situates itself in a complicated position between military and policing matters. Terrorism is both war and crime. Institutionally, this boundary often lies between different state agencies who must therefore cooperate and share data with one another. In the US as in most other countries, institutional rivalries and differing business practices between the likes of the FBI and CIA can mean that intelligence is not always shared as extensively and easily as should be the case. In many cases the problem might even be a simple yet infuriating one of having different databases that are not easily connected to one another.

The need to move intelligence across institutional boundaries extends further in the case of contemporary counter terrorism, from high-level state intelligence agencies all the way down to local policing bodies, since the connection between complex international intelligence and that from street-level community policing is increasingly central to the task. Much as notions of security have become broadened and more pluralistic since the end of the twentieth century, so the implications for security actors are that the picture has become wider, deeper and spatially more stretched in terms of who needs to be involved (Gill, 2006).

In practice, this makes the data-sharing picture even more complicated, since intelligence that may have been gained using highly sensitive techniques cannot always be shared very easily all the way down to the local-level police officer. Conversely, small scraps of information that local policing may come across in its daily work can often be extremely useful for the intelligence agencies in helping to contextualise what they are seeing, but often this information does not make its way up the information stack for a whole host of data recording and databasing issues.

At the level of tradecraft, Berkowitz suggests that the intelligence failure epitomised by the 9/11 attacks was also a failure of the Western intelligence machinery to re-orient itself from the “big and noisy” Cold War Soviet target to the low-signature world of Al Qaeda terrorism. There was also a concomitant failure in tradecraft whereby the old “case officer” model that had served well in Cold War embassies was finding itself of little use for the caves and fields of Afghanistan (Berkowitz, 2002). At a deeper level, there has also been a debate about whether Humint, which, as we have seen, is claimed by some to be the best and only way of effectively tackling a terrorist group (Jeffery, 1987) is realistically possible any longer when faced with a group such as Al Qaeda, which is far more difficult for Western agencies to penetrate for a host of cultural, linguistic and logistical reasons. Indeed, there is evidence to suggest that the initial intelligence successes against an organisation such as the PIRA, which was a traditional hierarchical organisation mirroring a state army, led to a decision to establish a flatter and more cellular structure from the 1970s onwards which could not be so easily penetrated (Bamford, 2005). This mirrors a similar evolution of large transnational crime groups, such as Colombian drugs trafficking cartels, which appear to have reorganised themselves into a much more dispersed and difficult target group following successful counter-narcotics operations in the 1990s (Kenney, 2003). It is certainly the case that one of the central challenges for counter terrorism agencies that Al Qaeda poses is its almost ephemeral and inspirational nature, which is very much at odds with the ways in which traditional terrorist groups were organised formerly.

Berkowitz’s conclusion on the Humint versus Technint point is a nuanced one: firstly, we should not throw up our hands at the complexities of the new threat and consider that Humint is now impossible. There have been some great difficulties in this area, notably the case of the triple agent Humam al-Bilawi, whose suicide detonation inside a US security facility at Khost, Afghanistan in December 2009, inflicted the CIA’s worst ever peacetime loss of life. For all such headline cases, we can reasonably assume there have been a number of Humint successes behind the scenes that have thwarted or disrupted potential attacks.

At the same time, technical intelligence gathering such as that from communications intercepts, for all its difficulties of language and code, are still going to be important in counter terrorism intelligence (Berkowitz, 2002). Indeed, Edward Snowden's revelations about the nature and extent of NSA and GCHQ's interception and data mining capabilities in recent years have only served to underline the seriousness with which the major intelligence agencies are viewing the development of cutting-edge Techint capabilities. Similarly, the keenness of governments such as that in the UK to enhance their data interception capabilities, and particularly the question of being able to move into the realm of internet-based communications, also underlines the continued significance of technical intelligence-gathering activities within the realm of counter terrorism.

In suggesting that the terror threat in the UK was at its highest level since the end of the Cold War, the head of MI5, Andrew Parker, recently focused on technical capabilities, by making the bold claim that it was no longer possible for the police and intelligence agencies to obtain all the communications about suspected terrorists that they need from traditional warranted access (Dearden, 2015). Clearly, governments suspect that a combination of diverse and obscure methods of communication over the internet, enhanced almost every day by the appearance of new applications and technologies, and coupled with the increasing ability for non-state actors to use sophisticated encryption methods, are going to make a serious dent in their ability to continue to collect intelligence on the key terrorist targets. Some of these challenges require expensive technical solutions, as Snowden has uncovered, while some will require legislative changes to allow the government to intercept and analyse more data than it can currently.

Complications and dilemmas

However, calls by governments to be able to enhance their legal and technical capabilities in the realm of the surveillance of internet-based communications, inevitably lead into a general public anxiety about the potential pitfalls of a Big Data world. Lyon describes a sort of "panoptic panic" that is increasingly entering the discourse in modern liberal democracies, whereby fears of "mass surveillance" (itself a concept misconstrued by the media in many situations) and potential abuses of power by governments, are looming large (Lyon, 2014). The MI5 chief's warnings about the level of terrorist threat in the UK, and the coupling of this warning with the need to enhance Techint capabilities, could be seen in a critical analysis as a form of official speech act that aims to ensure intelligence retains a central role in the discharge of counter terrorism policy, and continues to be resourced accordingly. Such warnings could be seen as evidence of Ulrich Beck's "risk society" (Beck, 2002). In Beck's analysis, prediction and risk are interrelated concepts: fear of the latter leads to an increasing desire for capability in the former, to attempt to block risks before they happen (Kerr and Earle, 2003: 68). Such pitfalls also underline the importance of trusted and reliable processes of parliamentary oversight of the intelligence agencies, such that the public can have trust in the government not exceeding its powers.

Orwellian fears of a Big Brother state, however, are not the only dilemmas faced by contemporary counter terrorism policy-makers in the post-9/11 era (Richards, 2012). The dangers inherent in "policing the underside of globalisation" (Aldrich, 2009: 29), in which contemporary international terrorism poses one of the archetypal threats, are not only present in requirements for complicated new interfaces between policing and national security agencies already described, but also put pressure on governments to work with a wider, and in some cases, more unsavoury range of international partners.

The case of Afghanistan's reconstituted intelligence agency, the NDS, has been a prescient one. As an important part of the security sector reform process in Afghanistan during ISAF's campaign from 2001 onwards, difficulties in dealing with an intelligence agency that has an extremely dark history from a human rights point of view has placed many of the ISAF partners in a perilous position. A number of accusations have arisen of systematic torture of suspects in NDS facilities (Gardham, 2010). In 2009, both Britain and Canada had to temporarily suspend handovers of detainees to the NDS when they were denied access to interview suspects in some Afghan facilities, suspecting that the suspects in question had been severely mistreated.

Such problems feed into the wider picture of extraordinary renditions and black facilities that seemed to be a feature of the immediate post-9/11 period, and which threaten to place Western powers in a seriously difficult ethical and moral position as the details emerge. There is no doubt that the aforementioned difficulties with Humint against contemporary terrorist targets have led Western intelligence agencies to widen the net of partner countries in the Middle East and beyond with whom they are prepared to have intelligence exchanges, since those countries will often have advanced Humint networks of their own in the relevant places and organisations. But this runs the risk of exchanging intelligence with regimes for whom torture and mistreatment of detainees is an established part of counter terrorism policy. The negative effects of this are twofold: firstly, the Western intelligence agencies and their governments are potentially placed in a very invidious ethical position, which can feed into radical anti-West narratives. Secondly, intelligence derived from torture usually leads to subsequent court cases collapsing and very substantial damages being awarded in order to avoid embarrassing exposure of sensitive material, with all the negative publicity attached. The case of Binyam Mohammed and his co-defendents, who ended up in

Guantanamo Bay and were eventually awarded "millions" in compensation in 2010 (Wintour, 2010), is an indicative case among many.

Back in the domestic scene, the elevation of community intelligence within counter terrorism policy can deliver its own complications. The logic behind community intelligence strategies for the police is fairly clear, not least as a successful police service has a wider need to be establish cooperative and supportive links with the communities it serves. The difficulties are that the state, through the police, must dance a difficult line between good community policing and accusations of spying on a particular "suspect community". As Heath-Kelly (2012) identified, there is also a contingent dilemma for the community itself, in that it can end up being both a critical friend and ally of the police in delivering security, and, at the same time, experience a degree of othering as a suspect community. There is some evidence that both Irish and Muslim communities have experienced such a dilemma at different times in the UK's history of terrorist threat. Moreover, in a major study of the effect of security policy on citizenship in the UK, Jarvis and Lister found amongst ethnic minority communities a "diminishment of citizenship that stems from anti-terrorism measures" (Jarvis and Lister, 2013: 672). The sense is that many in these communities feel they cannot fully participate in the political process since they are treated as othered, suspect communities without access to the key levers of power.

Policies such as Prevent in the UK have been shaped and reshaped a couple of times since its inception in 2005, reflecting the fact that this is a relatively new area of counter terrorism policy and will probably take several years to get right. In many cases the police have enjoyed good links with the relevant communities and have been able to disrupt and pre-empt a number of potential problem cases. But complainants such as Arun Kundnani see these programmes as sinister fronts for gathering intelligence on the Muslim community at large, and this can have serious consequences for inter-community relations, not to mention cause problems for intelligence gathering on terrorist threats (Kundnani, 2009). The moral hazards for any contemporary Western state in this area are wide-ranging.

Conclusions

There is no doubt that intelligence has been, and should continue to be an inescapable part of counter terrorism policy. As Frank Kitson famously said of counter-insurgency operations, "the problem of defeating the enemy consists very largely of finding him" (Kitson, 1971: 95). The same is true of terrorism today. Those planning terrorist operations are well aware that the state has a number of surveillance capabilities available to it, and that the terrorists will need to formulate their plans as covertly as possible if they are to be successful. The game for both sides is one of cat and mouse. It may be the case, as the PIRA famously informed the British government when it narrowly failed to assassinate the Prime Minister, Margaret Thatcher, in 1984, that the state has to be "lucky always" (Howard and Sawyer, 2002: 92). But the state can enhance its chances in the game by making sure it can obtain good intelligence on its foes.

The gathering of intelligence may be a morally dubious activity in essence. As the US Secretary of State, Henry Stimson said in 1929, intelligence is not something done by gentlemen (Shulsky and Schmitt, 2002: 169). At the same time, there could be an argument for intelligence-gathering having a strange sort of moral purpose and justification. This could apply on two levels. Firstly, as a former Permanent Secretary at the UK Ministry of Defence, Sir Michael Quinlan noted, it could be argued that some of the principles of "just war", such as actions of last resort to avert a major loss of life, could be applied to intelligence against the actions of terrorists plotting mass casualty attacks and thus given more than a little moral justification (Quinlan, 2007). Such sentiments were invoked by another British intelligence chief, Sir John Sawers, in a rare public speech when he was head of MI6:

> Most people go about their daily work not worrying about the risk of a terrorist attack. That a bomb may have been planted on their route, or hostages might be seized. I'm glad they don't worry about those sorts of things: part of our job is to make people feel safe.....You, and millions of people like you, go about your business in our cities and towns free of fear because the British government works tirelessly, out of the public eye, to stop terrorists and would-be terrorists in their tracks. (The Guardian, 2010).

Here, the intelligence chief is echoing the words of the UK's Counter Terrorism Strategy, which states that the aim is to reduce the risk from terrorism, such that "people can go about their lives freely and with confidence" (HM Government, 2011: 3). His speech included many positive words about his staff, such as "pride" and "commitment", which emphasised both principles of public service and a moral legitimacy in the work of intelligence in countering terrorism.

Secondly, historical experiences of the use of intelligence against terrorists is that it can deliver a safer and more effective outcome than would be the case in a "shooting war", in the sense that disruption and foiling of plots is better than having to confront terrorists in violent confrontations or deal with the aftermath of attacks. As the experience of the long war against PIRA showed, instances in which terrorist suspects were shot by Special Forces were relatively few: far more important over the years was the continual undermining and disruption of activities through intelligence actions. In this way also, rather than being an uncomfortable activity of moral dubiousness, intelligence might actually be an ethically sound and justified part of counter terrorism.

With all of that said, it is clearly the case that intelligence in counter terrorism scenarios faces many moral hazards and pitfalls. Arguably, the post-9/11 period and the process of globalisation that has run alongside are showing these risks to be wider and more complex than ever before. For states conducting intelligence in the contemporary era, a fine line must be walked between effective intelligence gathering to protect the security of citizens, and a host of ethical and reputational risks, the consequences of which can be deeply profound if the wrong choices are made for any government and its intelligence capability.

Bibliography

Aldrich, R.J. (2009) 'Global Intelligence Co-operation versus Accountability: New Facets to al Old Problem', *Intelligence and National Security*, 24(1), 26-56

Arce M, D.G. and Sandler, T (2005) 'Counterterrorism: A Game Theoretic Analysis', *Journal of Conflict Resolution*, 49(2), 183-200

Bamford, B.W.C. (2005) 'The Role and Effectiveness of Intelligence in Northern Ireland', *Intelligence and National Security*, 20(4), 581-607

Beck, U. (2002) 'The Terrorist Threat: World Risk Society Revisited', *Theory, Culture and Society*, 19(4), 39-55

Berkowitz, B. (2002) 'Intelligence and the War on Terrorism'. *Orbis*, Spring 2002, 289-300

Buzan, B., Waever, O. and de Wilde, J. (1998) *Security: A new framework for analysis.* Boulder CA: Lynne Rienner

Dearden, L. (2015) 'UK terror threat is at the highest level in 30 years and growing, MI5 chief warns', *The Independent* (September 17)

Fukuda-Parr, S. (2003) 'New Threats to Human Security in the era of Globalization', *Journal of Human Development*, 4(2), 167-179

Gardham, D. (2010) 'Britain 'hands over prisoners in Afghanistan to face torture'', *The Daily Telegraph* (April 19)

Gill, P. (2006) *What is Intelligence Theory?* In Treverton, G.F., Jones, S.G., Boraz, S. and Lipscy, P. (eds.) *Toward a Theory of Intelligence: Workshop Report*. Arlington VA: Rand

Guardian, The (2010) 'Sir John Sawyers's speech – full text', *The Guardian* (October 28)

Heath-Kelly, C. (2012) ‘Reinventing prevention or exposing the gap? False positives in UK terrorism governance and the quest for pre-emption’, *Critical Studies on Terrorism*, 5(1), 69-87

Herman, M. (2004) *Ethics and Intelligence after September 11*. In Scott, L.V. and Jackson, P.D. (eds.) *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*. London: Routledge

Howard, M. (2002) ‘What’s in a name? How to Fight Terrorism’, *Foreign Affairs*, 81(1), 8-13

Howard, R.D. and Sawyer, R.L. (2002) *Terrorism and Counterterrorism: Understanding the New Security Environment: Readings and Interpretations*. New York: McGraw Hill/Dushkin

HM Government (2011) *CONTEST: The United Kingdom’s Strategy for Countering Terrorism*. London: The Stationery Office

Jarvis, L. and Lister, M. (2013) Disconnected Citizenship? The Impacts of Anti-terrorism Policy on Citizenship in the UK’, *Political Studies*, 61, 656-675

Jeffery, K. (1987) ‘Intelligence and Counter-Insurgency Operations: Some Reflections on the British Experience’, *Intelligence and National Security*, 2(1), 118-149

Kenney, M. (2003) ‘From Pablo to Osama: Counter-terrorism Lessons from the War on Drugs’, *Survival,* 45(3), 187-206

Kerr, I., and Earle, J. (2013) ‘Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy’, *Stanford Law Review Online*, 66, 65-72

Kirk-Smith, M. and Dingley, J. (2009) ‘Countering terrorism in Northern Ireland: the role of intelligence’, *Small Wars and Insurgencies*, 20(3-4), 551-573

Kitson, F. (1971) *Low Intensity Operations: Subversion, Insurgency and Peacekeeping*. London: Faber and Faber

Kundnani, A. (2009) *Spooked! How not to prevent violent extremism*. London: Institute of Race Relations

Laqueur, W. (1985) *A World of Secrets: The Uses and Limits of Intelligence*. New York: Basic Books

Lyon, D. (2014) ‘Surveillance, Snowden, and Big Data: Capacities, consequences, critique’, *Big Data and Society* (July-December 2014)

Quinlan, M. (2007) ‘Just Intelligence: Prolegomena to an Ethical Theory’, *Intelligence and National Security*, 22(1), 1-13

Rapin, A-J. (2011) ‘What is Terrorism?’, *Behavioral Sciences of Terrorism and Political Aggression*, 3(3), 161-175

Richards, J. (2012) ‘Intelligence Dilemma? Contemporary Counter-terrorism in a Liberal Democracy’, *Intelligence and National Security*, 27(5), 761-780

Robertson, K.G. (1987) *Intelligence, Terrorism and Civil Liberties*. In Wilkinson, P. and Stewart, A.M. (eds.) *Contemporary Research on Terrorism*. Aberdeen: Aberdeen University Press

Sheehan, M. (2010) *Military Security.* In Collins, A. (ed.) *Contemporary Security Studies.* Oxford: Oxford University Press

Shulsky, A.N. and Schmitt, G.N. (2002) *Silent Warfare: Understanding the World of Intelligence*. Dulles VA: Potomac

Sims, J. (1995) *What is Intelligence? Information for Decision-Making*. In Godson, R., May, E.R. and Schmitt, G. (eds.) *US Intelligence at the Crossroads*. London: Brassey’s

Sun Tzu (trans. Griffith, S., 1963) *The Art of War*. Oxford: Clarendon Press

Thacher, D. (2005) ‘The Local Role in Homeland Security’, *Law and Society Review*, 39(3), 635-676

Von Clausewitz, K. (1982; original edition 1832) *On War. Book 1*. London: Penguin