The UK intelligence community before and after Snowden

Professor Richard J. Aldrich, University of Warwick

Department of Politics and International Studies (PaIS)

Report requested by the German Bundestag

Printed paper 18/843

18th electoral term 18.03.2014

Committee of Inquiry on Intelligence

The UK intelligence community before and after Snowden

Professor Richard J. Aldrich

Contents 2

Abbreviations

CIA	Central Intelligence Agency
Comsec	Communications security
DSMA	Defence and Security Media Advisory Notice System (DA-Notice)
Elint	Electronic intelligence
GCHQ	Government Communications Headquarters
IMP	Intercept Modernisation Programme
IPT	Investigatory Powers Tribunal
IRTL	Independent Reviewer of Terrorism Legislation
ISC	Intelligence and Security Committee, UK Parliament
JIC	Joint Intelligence Committee
MI5	Security Service
MI6	Secret Intelligence Service (also SIS)
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NSA	National Security Agency
NSC	UK National Security Council
OSA	Official Secrets Act
PSIS	Permanent Secretaries Committee on the Intelligence Services
RCUK	Research Councils UK
RIPA	Regulation of Investigatory Powers Act 2000
SAS	Special Air Service
Sigint	Signals intelligence
SIS	Secret Intelligence Service (also MI6)
TCG	Tasking and Co-ordinating Group
TPIMs	Terrorist Prevention and Investigation Measures
WIF	Warwick Intelligence Futures project
WMD	Weapons of Mass Destruction

The UK intelligence community before and after Snowden

1.Executive Summary

Few areas of public policy are more important than electronic intelligence and cyber-security. The revelations made by Edward Snowden have shone a bright light on this subject. The National Security Agency (NSA) and its many partners have grown rapidly, sharing data in a response to globalisation as well as terrorism. In an uncertain world, increased knowledge is often seems a security panacea. Whether global challenges are defined in terms of international terrorism, organised crime, disease or indeed demographic and socio-economic change, a common response has been to turn to knowledge-intensive organisations to manage societal risk. Today, the data derived from social media, from our travel cards and our supermarket loyalty cards, is at the core of this activity.

Government no longer owns most of this data. The most important change during the last decade is that “surveillance” has merged with “shopping” and has ceased to be the preserve of specialist state agencies; instead it has escaped out into society. The big collectors of intelligence are now the banks, airlines, supermarkets, ISP providers and telecoms. Every organisation, both public and private now collects, stores and shares data on an unprecedented scale - often across state boundaries. Airlines are typical of this new phenomenon as both vast collectors and also 'customers' of refined data for both commercial and security purposes. Are the organisations the future security agencies?

What are the consequences? In the UK the outcomes of these trends are often portrayed as darkly dystopian. Yet human beings are now more connected. Potentially, the new era of “knowledge-intensive security” offers stronger partnerships and more open styles of governance that will diminish government secrecy and corporate confidentiality as well as privacy. But this will require higher levels of trust regarding the way corporations and government handle personal data, together with “flat” ownership. We will also need radical new approaches and new concepts if oversight is to be improved and public confidence is to be sustained. The policy task is urgent, for while information and communications technology is accelerating, cabinets and corporate boards are often baffled by this subject.

Parliaments, the judiciary, human rights organisations and the media have also struggled to comprehend its potential and its dangers. In short, while the consequences of electronic intelligence and cyber security are important, they are as yet poorly understood and poorly regulated. Just like intelligence itself, oversight and the protection of rights is an activity that is increasingly dispersed. The lead elements are no longer formal committees but global civil society, consisting of a broad alliance of whistle-blowers, journalists, academics, campaign groups, lawyers and NGOs. These fluid international alliances of counter-spies work unevenly, but have the advantage of mirroring the multinational alliances of the intelligence agencies. National governments are not comfortable with “regulation by revelation” and have worked hard to constrain whistleblowers. But if the UK government wishes to recapture the inactive in this difficult retrain it will probably have to follow the advice of David Anderson, the UK Independent Reviewer of Terrorism Legislation and opt for judicial review of intercept warrants. It will also need a more effective mechanism for reviewing international intelligence co-operation.

2.Task

The task is to consider how within the United Kingdom in the Parliament, in the mass media, and in the academic society the following subjects are being discussed:

1.The pursuit (performance, execution) of UK intelligence agencies.

2.The parliamentary oversight of intelligence agencies.

3.The protection of privacy and civil liberties in the UK.

4. This needs to be considered within the framework of a different set of questions posed by the inquiry. I have also tried to address these, while also conscious that these wider questions are not my immediate remit.

5. The conclusion draws out some of the wider global and technical context within which UK intelligence and security is changing and offers some limited prescriptions.

3.Approach, sources and methods

There are ample reports and summary accounts that describe the UK intelligence and security agencies, together with their oversight and regulatory mechanisms. By contrast this report seeks to offer advice and commentary drawing on the wide-ranging debate on these matters that has been ongoing in the academic community since the 1980s.

Academics in the UK have been researching intelligence and security services for over three decades (Andrew and Dilks 1984). Accordingly, some of the responses offered here reflect data gathered over a long period. Other responses draw on the Warwick Intelligent Futures (WIF) project and a forthcoming book on the UK core executive and intelligence (2016). Between 2008 and 2012, Warwick hosted two AHRC project in partnership with the University of Nottingham and this report makes use of those findings. There has also been additional research conducted to respond the questions posed by this inquiry over the summer of 2015. This is an academic analysis that seeks to set UK developments in their broader context, together with some observations about future development over the next decade. It might be helpful to state that I do not hold a security clearance and I therefore do not enjoy privileged access to classified information.

4.Ethics

In conducting research for this inquiry and on any other related projects, I have at all times been mindful of research ethics. I have followed the guidelines set out by Warwick University Research Ethics Committee and the UK Research Councils Policy and Guidelines on Governance of Good Research Conduct (RCUK 2015).

5.The End of Intelligence?

The twenty-first century will be defined by "big data", greater mobility and personal connectivity. The speed and scale of change is impressive. IBM has estimated that 90% of the world's data was created in the last two years. In 2012, the world sent over eight trillion text messages. In five year's time, everything we buy in a shop that costs more than ten Euros will have an IP address and will collect information on the world around it. Many farm animals now contain SIM cards that transmit their health status and in ten year's time, equivalent body-monitoring for humans will be ubiquitous. In twenty year's time we will think - then blink - and send an email. In cities like Berlin, London, New York and Toronto the majority of human interactions will be recorded. Not only will this data be of unimaginable size, it will be increasingly accessible from mobile devices that are ever more closely integrated with the human body and eventually the human mind. Who will secure these digital shadows of ourselves? And will they constrain us - or make us more capable and free?

In an uncertain world, increased knowledge is often held out as a security panacea. Whether security challenges are conceived in terms of traditional battlefield combat (which is by no means a thing of the past) insurgency and international terrorism, organised crime, peacekeeping or humanitarian relief operations, a common response has been to turn to knowledge-intensive organisations that deploy "big data" to manage risk. Moreover, as the majority of operations have moved down the spectrum towards what General Rupert Smith has called 'war amongst the people', intelligence is increasingly about human beings (Smith 2007). Today, human beings emit what the CIA has called a constant stream of 'electronic exhaust fumes' as they live their lives, the data derived from sources as mundane as tweets, supermarket loyalty cards or gaming chat-rooms are transforming intelligence and opening the door to what we might call "knowledge-intensive security".

One of interesting aspects of this process is the changing ownership of information. Once upon a time, data of interest to intelligence agencies was primarily in the government domain, but this is gradually changing with a shift to a security focus on intra-state war, insurgency and the crowd. The most important change during the last decade is that "surveillance" has merged with travelling and shopping. It has ceased to be the preserve of specialist state agencies; instead it has escaped out onto the Internet and even out into society more broadly. Big collectors of intelligence that interests the security agencies include the banks, airlines, supermarkets, ISP providers and the telecoms. Many organisations, both public and private, now collect, store and share data on an unprecedented scale - often across state boundaries. Airlines and airports are good examples of "dual use" intelligence partners, given that they are both vast collectors and also 'customers' of refined data for commercial, security and military purposes.

What are consequences of a world driven by "big data"? The outcomes are disturbing and certainly subversive of familiar and reassuring categories. The boundaries between intelligence and information, between openness and secrecy, also between private and public all appear to be corroding fast. But there are also exciting opportunities for a new public-private partnerships and enhanced accountability. Cyber-security offers the best example. Here, recondite government agencies whose names were unknown to the public even a decade ago are openly and successfully engaging with every sector of society in order to protect our electronic infrastructure. Intelligence and security agencies may be required to explain their missions more freely and frankly. We may be moving towards what David Brin calls "The Transparent Society" in which both secrecy and privacy change radically with significant potential benefits for the state, the corporation and the individual citizen. Individual privacy, corporate confidentiality and government secrecy are all in decline and much will depend on how the resulting data is owned (Brin 1999).

In an ideal world, both the intelligence power of state agencies as a force for good and the oversight capabilities of their regulators will benefit from the fact that human beings are now more connected, indeed are increasingly addicted being in "constant touch" (Agar 2003). Potentially, the new era of "knowledge-intensive security" offers stronger partnerships and more open styles of governance. But this will require higher levels of trust regarding the way all sorts of corporations and defence bureaucracies handle personal data. We will also need innovative approaches and new concepts if public confidence is to be sustained. The research task is urgent, for while information and communications technology is accelerating, cabinets and corporate boards are often baffled by it. Parliaments, the judiciary, human rights organisations and the media have also struggled to comprehend its potential. In short, while the economic, social and political consequences of "big data" might well be beneficial, they are as yet poorly understood by the majority of those involved in security governance.

Knowledge-intensive security also has complex implications for intelligence and security bureaucracies because it connects intelligence to other knowledge intensive activities, ranging from energy and transport to medicine and social services. We need to ask much more open-minded questions about the social implications of knowledge-intensive security. Can knowledge-intensive security promote a more open and flexible approach to public security operations? What role will corporations play and what are the implications for the defence economy? How will the security of knowledge-intensive systems be governed nationally and internationally? How will public confidence and trust in knowledge-intensive systems be sustained when they are deployed by the state? Finally, and most importantly in the wake of the "Snowden crisis", what are the implications of knowledge-intensive security for civil rights and national security law?

Intelligence needs to connect transforming technologies with the social aspects of information to contribute a 'new vision' of its role that is based more than consent and partnership. This will require advanced research and a range of methodologies drawn from the social sciences and the natural sciences. There is considerable potential here. Knowledge-intensive security will not only shape the future of military affairs, global business and modern society, it will also ensure that they are more connected, often in unexpected ways. In the next decade "big data" will pervade every aspect of our lives. Understanding how digital assets can be protected from crime and used positively to increase effectiveness will enhance our opportunities for a prosperous and sustainable society. But the challenges to intelligence are immense as technology continues to accelerate and our societies become ever more focused on data.

Nevertheless, working together, the universities, the major ISP and defence bureaucracies have strength in depth here and have the potential to deliver creative thought around the issue of knowledge-intensive security. We require greater interdependency between people, organisations and nation states in order to successfully manage risk, ensure consent and achieve credible oversight. Progress will require not only an ability to anticipate obvious threats but also an ability to understand long-term changes in the wider realms of governance and society and how both of these interact with technology.

Intelligence and security agencies now inhabit what Joshua Rovner has called "the Twitter Age" (Rovner 2013). We are not only seeing radical changes to intelligence, perhaps even the end of intelligence as an old-style discreet and compartmentalised discipline, was are also seeing a diminution of secrecy, not least because new intelligence practices are spawning additional oversight through a demassified media. Paradoxically, while the new social ecology of intelligence has made public confidence and trust ever more important, this transition has taken place against the background of a series of events that have damaged public confidence in intelligence. These include the Iraqi WMD fiasco and practices conducted within the boundaries of the European Union which CIA officials have themselves described as torture (Allen & Foster 2015).

Partly as a result of this, "whistle-blowers", human rights campaigners, NGOs and journalists have over-taken political bodies as the main form of over-sight and are increasingly suspicious of big data and even perhaps technophobe in their world view. There are major research challenges here and we still know relatively little in quantitative terms about social attitudes to intelligence across European society, business and even within broad swathes of government itself. We certainly need to move our ideas about intelligence beyond the familiar setting of government institutions.

6.The End of Secrecy

During the summer of 2013, Edward Snowden leaked remarkable details of several highly classified US/UK surveillance programmes to the Washington Post and the Guardian, sparking an international furore. Snowden was vilified and applauded in equal measure. Officials in London and Washington regard these latest disclosures as the most serious breach in government security for several decades. The media have framed this episode around surveillance and civil liberties, focusing upon 'the end of privacy'. Certainly, there has been a degree of moral panic with governments allegedly able to monitor every aspect of our digital lives. However, the changing nature of privacy for the citizen is only part of the picture and these developments also denote a 'crisis of secrecy' for government. For many officials in London the most alarming issue is not government looking at us - but us looking at government.

Snowden is symptomatic of something much bigger. All governments are increasingly concerned by large-scale and unauthorised releases of classified documents facilitated by disaffected officials who are often described as "whistle-blowers"'. Bureaucracies invest considerable resource in protecting secrets and in the USA the annual cost of classification is estimated at $11 billion (Shane 2011). This is a shadowy world and while governments have deployed remarkable technologies in an attempt to track leakers and the journalists they work with, we still know relatively little about procedural secrecy and its opponents. This is a technical war that precedes Snowden and has in fact been fought with increasing bitterness since 9/11.

New technology is central to this process. Ten official whistle-blowers have come to public attention in the last decade beginning with the GCHQ employee Katherine Gun in 2003. However, more recently, websites such as WikiLeaks have deployed anonymising software to allow officials to release very large collections of documents, in collaboration with several mainstream newspapers. In November 2010, the website leaked more than 250,000 US diplomatic cables, exposing the frank views of officials on a wide range of current international issues. As Heather Brooke, the journalist who exposed the UK parliamentary expenses scandal, observed in the wake of this – 'the data deluge is coming' (Brooke 2010).

The results are revolutionary. Governments now confront a cultural challenge around new forms of oversight and accountability. Internet activists and digital whistle-blowers claim that their purpose is a new form of horizontal regulation secured through the democratization of information. In the "twitter age", the use of blogs and social networks are allowing journalists to mount lengthy investigations that rival those of scrutiny committees deployed by elected bodies. The lead in terms of deep investigation of government security activity may be passing from formally constituted commissions and committees towards a version of global civil society, characterised by NGOs, civil rights lawyers, journalists and regional bodies such as the Council of Europe.

To some extent this has always been the case. Harry Howe Ransom described journalists as 'the shock troops of accountability', capturing the way in which press investigation of the CIA had paved the way for a veritable season of inquiry on Capitol Hill during the early 1970s (Johnson 1986). But arguably two things have changed. Back in the 1970s, Daniel Ellsberg required twenty-four hour access to photocopiers in order to leak the "Pentagon Papers" - but now disgruntled officials can release entire archives of secret material with a pen drive. Direct access to high volumes of highly-classified data has allowed leakers, whistle-blowers and journalists to overtake formal oversight bodies as the lead element in accountability. Who would read the redacted and censored reports of the UK Intelligence and Security Committee when one can read Luke Harding's analysis in the *Guardian* with links to original GCHQ powerpoints?

For parliaments and assemblies, the regulatory questions around whistle-blowing and secrecy are in many ways just as important as the regulation and oversight of the intelligence and security services – and they are fundamentally connected. Both the United States and the Europe Union are investigating "Whistle-blower Protection", raising important normative issues around where the line should be drawn between the public right to know and the right of civil servants to offer confidential advice to ministers. Snowden has placed officials in Whitehall and Washington on notice, and new conventions around what remains of secrecy will need to be put in place.

Discussions between America and Europe on these matters have been underway for almost a decade. The trigger was the issue of renditions and secret prisons in Europe. In November 2005, path-breaking reports in the *Washington Post* by Dana Priest revealed the existence of CIA 'secret prisons' in 'several democracies in Eastern Europe' holding high-value detainees. The disturbing idea of secret prisons on European territory was the initial point of departure, but EU institutions soon interested themselves in wider issues such as the "ghost flights" that had made their way through European airspace carrying detainees to far-flung destinations. They also looked at the possibility of extraordinary renditions from European countries such as Sweden, Germany, and Italy to countries outside the EU with dubious human rights records (Priest 2005).

The Council of Europe's Committee on Legal Affairs and Human Rights of the Parliamentary Assembly took the lead. The Rapporteur, Swiss Senator Dick Marty, enjoyed only limited resources for his inquiry. However, he was assisted by the Secretary-General of the Council of Europe, who employed his power under Article 52 of the ECHR to request information from member states as to how their laws provided protection against secret detention (including by foreign states) and asked for details of recent instances. In March 2006, the Venice Commission issued a legal opinion concluding that participation in secret detention is not compatible with ECHR. Remarkably, the Venice Commission asserted that signatories are not only required to avoid such practices themselves, but also obligated to act to police such activity by partner intelligence services within the boundaries of Europe, a requirement that has had profound implications. The European Parliament carried out its own inquiry into renditions, reporting in November 2006, and the European Commission then conducted a third inquiry, reporting in November 2007 (Hakimi 2007).

These inquiries were important in three respects. Firstly, they underline that many respected lawyers now feel that *national* oversight mechanism are ill-equipped to investigated what are increasingly multinational intelligence operations. Secondly, it underlined the extent to which secret operations were nevertheless vulnerable to investigations for a multitude of open sources, including records collected by plane-spotters. In the wake of this episode, one senior CIA officer observed 'We no longer have secrecy, all we have is delayed disclosure' (CI). Thirdly, and most importantly it prompted a number of government officials and agencies in Europe to press the Americans to tighten up on secrecy and especially upon journalists. The response of the Americans was that constitutional constraints made anything like a UK Official Secrets Act impossible. However, they did undertake to tighten up on journalists by pursuing their sources and prosecuting them with vigour. This secret agreement was reached during 2006 and 2007 as part of a transatlantic renegotiation of the West's counter-terrorism strategy (CI).

Barack Obama's administration has prosecuted more leakers than all the precious US government put together. Obama has been even more energetic than George W. Bush in seeking to use the courts to punish government whistleblowers and to bring pressure to bear on journalists who work with them. One the most important aspects of Obama's national security strategy has been a firm determination to make secret programmes more secret still, and to avoid further leaks. This is underlined by the thirty-five year sentence imposed on Chelsea Manning, the source of the State Department cables obtained by Wikileaks, and the decision to charge Snowden with espionage (Harris 2012).

In part, the 'end of secrecy' problem has been accelerated by government. Intelligence, and indeed security agencies in general, have themselves radically undermined a central pillar of secrecy. The 9/11 attacks were followed by a cultural shift across the Western intelligence community which has been described by GCHQ as the shift from "Need to Know" to "Need to Share". Global terrorism and global organised crime increasingly lived in the seams of national jurisdictions and therefore required greater cross-governmental connectivity - the maxim of the day was, 'Play well with others'. Some have argued that this sharing and intelligence inter-activity went too far, the result being that security clearances were given to excessive numbers of people. Both Manning, a lowly Private First Class, barely into his twenties, and Snowden, a temporary contractor also in his twenties, had access to hundreds of thousands of documents from classified servers. We have seen a deliberate weakening of internal boundaries within government and also boundaries between the security agencies and their burgeoning army of logistical and technology contractors in the private sector (Priest and Arkin 2012).

Intelligence is fighting back. It has adopted a more forward strategy of information control to protect its reputation (Aldrich 2009). We have heard government public relations staffs talk about "nation-branding". Is it too adventurous to talk about efforts at "intelligence–branding" in the future? As early as 1996, a number of expert commentators and lawyers postulated a new information management strategy whereby information control is presented as greater openness and security agencies offset damaging leaks by accelerating their own efforts in the realm of public relations (Gill 1996, Moran 2013). Some argue that this has been exemplified by the recent UK authorised histories of the Security Service and the Secret Intelligence Service and by the CIA's adventures with film through Zero Dark Thirty (Andrew 2009, Jeffery 2011). In April 2014, the UK government announced the appointment of an official with a background in public relations as the new Director of GCHQ, Robert Hannigan. All this is part of the new infosphere of "knowledge-intensive security" and we will need to develop a new ideas around government attempts to manage public expectations in terms of declassification and openness.

7.The pursuit (performance, execution) of UK intelligence agencies.

7.1 Overall Trends

How do the UK intelligence and security services deliver their mission? How do they seek to achieve efficiency and effectiveness? How have they changed in the face of the challengers posed by the attacks on America and Europe between 2001 and 2005? This section considers developments in the UK security state, examining the intelligence and security services, together with the Whitehall machinery that connects these agencies with the core executive. It will also consider related aspects of security policing or 'high policing'. It seeks to interpret the major developments that have taken place since the end of the Cold War against the background of Europeanisation, globalisation and the so-called 'Global War on Terror'. The discussion will address some of the more important legislative changes that have ushered in mechanisms for oversight and a remarkable new culture of regulation. More broadly however, it is important to emphasise that during the last two decades, the UK security state has undergone three major changes -

a) **Hitherto secret parts of government have witnessed unprecedented exposure.** During the 1980s the very existence of the bodies like the UK Secret Intelligence Service (MI6) was often denied by a government characterised by obsessive secrecy. Europe was the main agent for change here. Legal actions brought before the European Court propelled many countries, including the UK, to avow their agencies, to place them on a firm legal basis and to institute oversight mechanisms. By 1994, Whitehall had begun to make virtue of necessity, talking of Open Government and employing web sites for personnel recruitment for the Government Communications Headquarters (GCHQ). This shift towards a higher public profile accelerated with the debate over intelligence prior to the Iraq War. By 2005, inquiries into intelligence and WMD transformed what had been a gentle limelight into a harsh spotlight. When John Scarlett took up his new post as Chief of MI6 at Vauxhall Cross, his face was well known and his track record was actively debated in the broad-sheet press.

b) **The UK intelligence and security services have ceased to be passive watchers and have instead become fixers, enforcers and “event shapers”.** The most important factor here has been globalisation. The Cold War had mostly required the secret services to focus largely on the passive observation of a relatively static enemy (with the exception of Northern Ireland). By 1995, the liberalisation of economies, together with the impending expansion of Europe, had increased anxiety about transnational crime. Statistically, organised crime was a larger threat to life than either war or terrorism and was increasingly regarded as a security problem in its own right. This prompted the creation of a new agency, the National Criminal intelligence Service (later the Serious Organised Crime Agency) in April 2006. It also drove a shift towards intelligence-led policing and towards security agencies that would not only observe but also disrupt harmful activities. This trend was already evident in 1999, but the upsurge in terrorism has completed a transformation of the security agencies. MI6 increasingly prides itself on low impact covert action and information operations which it describes as “event shaping”.

c) **State intelligence has expanded and its extent is now uncertain.** The size of the UK Security Service (MI5) has broadly doubled, reaching some 4,000 in 2008. The old Special Branch has largely been replaced by anti-terrorist police and special operations police located in regional hubs that also enjoy an agency/military presence. MI6 and GCHQ are also growing, with the latter now too large for their new building. Many government departments and also local government are engaged in counter-radicalisation and gather intelligence on possible extremism. There are also important public-private partnerships with GCHQ and MI6 out-sourcing its work to trusted companies often run by ex-government employees. Moreover, all elements of government are now empowered to conduct 'covert operations'.

Increased size has consequences for complexion and character. One of the historic virtues often claimed for the UK security state is that it is small and operates as a genuine community. Senior staff have tended to be long-term professionals rather than political appointees (unlike the United States) and are known to each other. However, the UK's expanded security state poses new challenges in terms of co-ordination and management. This has been addressed by creating a growing number of inter-agency working groups and teams, together with thematic analytical bodies dealing with issues like terrorism and cyber threats.

7.2 The Cold War

The UK security state is still a legacy organisation that reflects its heritage. The most venerable component is the police Counter-Terrorist Branch (SO16) whose origins lie in the 1880s. The UK's lead security element consists of the Security Service (MI5), created in 1909 in response to largely fictional anxieties about German espionage. Their main Cold War opponents were the Soviet Bloc espionage services whose human agents achieved remarkable success in gathering intelligence, albeit their masters proved incapable of making effective use (Andrew & Mitrokhin 1999). The Cold War and the rise of ideological conflict introduced concomitant anxieties about 'subversion' and this in turn led to the expansion of political policing.

MI5 activity also involved a process of background checks on UK citizens engaged in sensitive government work, referred to as 'vetting'. The volume of individuals vetted was high and included policy-makers in Whitehall, researchers at Aldermaston and even non-government staff in the arms industry. Vetting was introduced under strong American pressure following the discovery of Soviet moles, including the atom spy, Klaus Fuchs. This was one of the last initiatives of the Attlee government. During the 1960s and 1970s fear of Soviet penetration in both Washington and Whitehall was intense, leading to the "bugging" of Downing Street. Security measures included background checks on BBC employees who were sometimes debarred from promotion for fringe political activities. Controversially, potential ministers could also be blacklisted. MI5 maintained files on Jack Straw, the most senior and experienced cabinet minister of the last decade, and also Peter Mandelson, as a result of his youthful political activities (Sunday Times 1996; Barnett 2002, 376-7).

The end of the Cold War took the UK's security agencies by surprise. It was not predicted by the UK's main intelligence analysis body, the Joint Intelligence Committee (JIC), nor indeed by the intelligence agencies of its allies. Although this resulted in budgetary cuts of some 25% for the UK security agencies, they did not suffer the sort of psychological crisis that gripped their American counterparts. After 1989, the IRA was still active and spare resources were re-directed towards Northern Ireland. In 1992, MI5 were given overall responsibility for intelligence on the IRA on a world-wide basis. Moreover, the need to maintain a watch on some extremists groups and to maintain databases to support vetting remained. During the 1990s the focus moved to single-issue groups and by 1999, militant Islamic groups (Lustgarten and Leigh 1991, 613-642).

7.3 Northern Ireland

The UK security state has enjoys a reputation for joined-up government and integration with the core executive. However, this did not occur in Northern Ireland where six different intelligence and security services spent the first decade of the troubles tripping over each other. For most of the

1970s there were over 250 deaths each year and it was only in the 1980s that this fell significantly. Gradual penetration of the paramilitaries, together with the deployment of a vast range of surveillance technology deterred an increasing proportion of the planned attacks. In part this required the UK to build a large corps of intelligence officers who were skilled in running covert operations, a process which typically takes a decade (Gearty, 1991, 123). Proper order was not imposed on intelligence in the province until the mid-1980s with the creation of six regional Tasking and Co-ordinating Groups (TCGs) which had full oversight of all covert operations in a particular area. The current UK National Intelligence Model employed by the UK police makes use of TCGs and other lessons learned in Ireland and one might argue that the current regional Counter-Terrorism Units reflect the same thinking.

Contrary to Margaret Thatcher's assertions about 'not talking to terrorists', the UK was engaging with the IRA continuously through MI6 officers based in Dublin. Latterly, this eased the way towards a political settlement in Northern Ireland during the 1990s. Declining IRA activity was felt most keenly by MI5. Having taken the lead on Irish terrorism following the end of the Cold War, it was now losing another area of core business. To keep it alive, the government took the extraordinary step of handing MI5 some responsibility for intelligence support on organised crime after a process of minimal public consultation in the 1990s.

Many current aspects of security had their antecedents in the 1990s. IRA attacks on the City of London in 1992 and Canary Wharf in 1996 signalled a new anxiety about strategic terrorism that threatened national infrastructures, economic well-being and raised worrying questions about resilience. The response also pointed the way towards public-private partnerships in security. A 'Ring of Steel' was thrown up around the City of London reflecting a network of agreements between government agencies, private security companies and the financial institutions. Operation Griffin not only helps to train private security operatives employed by the banking houses, but also permits the exchange of intelligence between public and private partners. Some of the communications infrastructure for Griffin is provided by banks rather than by government networks. 'Griffinisation' - the development of public-private security partnerships - has accelerated (London Assembly 2005).

It is often assumed that Northern Ireland is no longer a security concern for the authorities. In fact a sizeable terrorist threat remains from dissident elements amongst the paramilitaries and there was a noticeable spike of terrorist activity in 2010. Northern Ireland has imprinted itself deeply on the operations of both the security agencies and the Army. However, since 2001, Cabinet Ministers have been reluctant to permit the sort of patient long-term penetration operations that were typical as late as the 1990s. The threat of mass casualty terrorism has resulted in a risk–averse approach and a tendency to ‘see and strike’ rather than to ‘watch and wait’.

7.4 Globalisation

The common perception is that the current activities and operations of the UK intelligence and security services are shaped by counter-terrorism. In fact, since the end of the Cold War, the main changes instead reflect broader developments in the international system which relate to 'globalisation'. Globalisation is most commonly associated with deterritorialisation and assertions of the decline of the sovereign state, together with notions about the communications revolution as an accelerator of these processes. For the UK, globalisation has perhaps been most significant in economic terms. The UK deregulated faster than most other European states and gained visibly from the expansion of world trade and the financial services industry. This is symbolised by the growth of London as a major financial capital and the emergence of its airport as the world's largest air transport hub. During the early 1990s, few in government viewed globalisation as anything other than unqualified good.

Al Qaeda thrived on globalisation and this group emerged just as the intelligence capacity to address it was being curtailed drastically as the result of post-Cold War cuts. Moreover, the 1990s saw the rise of separate but connected challenges, many of which might be described as complex clandestine networks. They included narcotics, money laundering, people-trafficking, war-lordism, nuclear proliferation and the illegal light weapons trade. These problems were accelerated by globalisation and over-lapped with "New Wars" of which the former Yugoslavia was the most prominent. In Russia, the Balkans and Central Asia, a range of shadowy figures from the security services were also major players in the criminal underworld. As a result MI6 moved from an emphasis on country stations to a more flexible format with mobile teams and shorter term deployments (Kaldor 2013).

The common element among these new threats was that many of them operated clandestinely. By the late 1990s the UK government was reversing the cuts in the budgets of the security agencies (Rice and Thomas 1997, 14-15). The shift in emphasis was confirmed by a summit at 10 Downing Street in late 1999 attended by MI5, MI6 and GCHQ which authorised a significant diversion of their resources against organised crime. In June 2000, the shocking discovery of fifty-eight Chinese illegal immigrants who had perished in a container lorry at Dover highlighted the seriousness of these issues. Crime was increasingly reconceptualised as a security problem to be addressed through intelligence. In part this reflected the planned expansion of NATO and the European Union, giving the UK an open frontier that extended as far as the Urals (National Criminal Intelligence Service 2000; Barnett 2002, 366-7).

Globalisation has been intimately associated with the retreat of the state. In the UK this has manifested itself in terms of deregulation and privatisation. The UK's new dependence on financial and service industries has also required concerted attention to critical national infrastructure. In the 1990s, the new priority was to guarantee secure e-commerce. This required a major culture change for the UK security state. Hitherto the security of communications infrastructure had been conceived largely in terms of government agencies. The work-a-day security of government cyphers had been protected by Communications Electronic Security Group (CESG), the defensive arm of GCHQ in Cheltenham. However, during the late 1990s there was a growing realisation that government would need roll out the same level of protection to banks and businesses who had become increasingly reliant on the internet. Moreover, many activities that had been state-owned, including the UK's telecom infrastructure itself, had been privatised. Accordingly, by 1997 the CESG transformed itself from a secretive entity into a national technical advisory service with a public face, setting standards for encryption and offering support to business on a cost recovery basis.

However, its activities have remained controversial, since many question its interest in encouraging the independent growth of truly secure systems. Within both NSA and also within GCHQ there has been a longstanding tension between those who emphasise defensive security and those who priorities weakening systems for the purpose of offensive penetrations. This debate has now become intense, partly because of the increasing dependence of much of the UK transport and energy infrastructure on the internet and also because of the rise of cyber-war. Many officials at GCHQ are uneasy about what they perceive as an American emphasis on the militarisation of cyber space as the fifth dimensions of warfare. Anxious debates are now proceeding about vulnerabilities in the UK national infrastructure and assessing just how much protection they need is arguably a new discipline intelligence (CI).

Officers at GCHQ have described MI5 and MI6 as 'the tiddlers' or little fish. GCHQ has always been the intelligence giant in the UK and constitutes the largest and most expensive element in the UK security state. Its size and extent is hard to quantify and assessing its budget is especially hard. Typically, GCHQ makes sizeable use of parts of the UK's defence infrastructure including satellites and submarines. Should these sorts of things be "costed in"? If we did so, the real cost of GCHQ in 2015 might be thought to stand at around £3 billion per year. Increasingly we have seen the state try to legislate away the costs of GCHQ by imposing statutory burdens on the ISPs and telecoms in terms of storage and access.

GCHQ's biggest moment of crisis was the mid-1990s. The exponential increase in global communications traffic, together with new modes of communication, presented severe challenges. Meanwhile a Treasury-inspired review under Roger Hurn in 1995 cut its budget by 25%, reflecting a demand for a post-Cold-war dividend. The following year, under the direction of David Omand, much of the old Fordist organisational structure was abandoned. Modelling themselves on leading business corporations, they undertook a management revolution, which resulted in flatter hierarchies, flexible teams and greater knowledge sharing. Its Mechanical Engineering Division was entirely privatised. This was followed by a decision to invest in cutting edge technologies under a programme entitled Signals Intelligence New Systems (SINEWS). Emblematic of this change was the move to a vast new GCHQ building on a PFI basis, completed in 2003. At the time, GCHW anticipated that it would only occupy 2/3 of the building, leasing the rest out. It is now too small to accommodate GCHQ's operations. After 9/11, much of the new resource available from counter-terrorism was invested in addressing the internet.

7.5 "New Terrorism" and 9/11

During the late 1990s, the UK security state was gradually becoming aware of what some have called the "New Terrorism". This was characterised by religious motivation and ambitious attacks together with new organisational structures and operations that took advantage of globalisation. The physical manifestation of this was the exodus of trained foreign fighters from Afghanistan after the end of the Western-backed war against the Soviet occupation. There was also growing concern about the interaction between terrorism, proliferation, failed states and organised crime. The UK Terrorism Act of 2000 addressed this, providing a wider definition of terrorism which included political, religious or ideological causes and also covered activities outside the UK. This increased police powers relating to stop, search and detention and empowered stronger financial investigation. In the wake of a peace settlement in Northern Ireland, some found it odd that special provisions were being expanded rather than dismantled. However, these changes anticipated future trouble (Moran 2006, 343). After the 9/11 attacks the UK government moved to implement new counter-terrorism strategy entitled 'Contest'. 'Contest' consisted of four main strands:

- Prevention: addressing the underlying causes of terrorism both here and overseas through, for example, support for moderate Islam;

- Pursuit: using intelligence effectively to disrupt and apprehend terrorists, with increased joint working and intelligence-sharing internationally, tightened border security and new measures to target identity theft and terrorist finance;

- Protection: using protective security precautions to minimise risks to the UK public at home and abroad; and

- Preparedness: improving resilience to cope with terrorist attacks or other serious disruption.

It is possible to argue that we have seen a fifth and more secret "P" in the form of "pre-emption" that reflects government anxiety about large-scale attacks and the potential use of unconventional weapons. The UK security state is much less willing to allow potential terrorists to remain at large. Over the years, and reflecting its experiences in Northern Ireland, the UK had developed an intelligence strategy towards terrorism that might be described as 'watch and wait', hoping that terrorists who remained at liberty would continue to give off valuable intelligence. Since 9/11, the UK strategy has increasingly leant towards 'see and strike'. This has a damaging effect on the flow of intelligence, scene once suspects are incarcerated, the information they can offer under integration quickly becomes outdated (Omand 2005, 107-116).

The UK core executive also changed in the wake of 9/11. In June 2002, the post of Intelligence Co-ordinator in the Cabinet Office was upgraded to become a Second Cabinet Secretary with wider responsibility for Intelligence, Security and Resilience. The addition of 'resilience' greatly expanded the role and reflected Sir David Omand's desire to encourage joined-up government with many departments that had hitherto given little thought to resilience or security (Omand 2004, 26-33). The traditional view that security was the responsibility of specialist sections of government was at an end. This was reflected in a new mechanism for processing operational intelligence on terrorism, an all source fusion centre called the Joint Terrorism Analysis Centre, located within the MI5 building at Thames House. This consists of participants from many different departments together with outside experts and academics. Its inclusiveness has been widely praised and it has been emulated across Europe. MI5 itself has taken on an expanded co-ordinating role for a range of national security activities that go far beyond its traditional roles and includes infrastructure – even the storage of farm yard fertilizer (Bamford 2004, 744-5).

New powers also arrived. Most controversial was the new Anti-Terrorism Crime and Security Act of 2001 which extended police powers against suspects (Fenwick 2002). The authorities were quick to use the new powers granted in 2000 and 2001 to arrest demonstrators who clearly had no relationship to terrorism, typically peace protestors outside an arms fair in London. In one case the police served a Section 44 Order (anti-terrorist order) on an 11-year old girl. Similarly, the US Department of Justice has conceded that the Patriot Act has been little used against terrorism, but has proved more useful against drug trafficking and organised crime. This reflects a deliberate corrosion of the boundary between intelligence and criminal investigation. The most obvious example of this in the UK has been use of intelligence presented to secret tribunals regarding immigration, detention or control orders. This material is of variable reliability and yet it is difficult to challenge (Moran 2006, 342, 345; Wada 2002, 51-9).

The 2001 Anti-Terrorism Crime and Security Act allowed a significant number of people to be held indefinitely without charge by derogation from ECHR. For many, this recalled Ulster's dubious era internment under the Special Powers Act of 1972. By February 2004, some fourteen individuals were held under these provisions and kept at Belmarsh Prison. These were non-EU citizens detained on the basis of secret dossiers that often catalogued their associations rather than their activities. Returning to their country of origin was the only alternative to permanent detention. The following December, a nine-member bench of the House of Lords ruled this to be a contravention of their human rights. This system has been replaced by restraining orders that are akin to house arrest and yet more recently by "TPIMs". Under further legislation passed in 2002 the Home Secretary gained the power to revoke citizenship (Bamford 2005, 748-9; Chirinos 2005, 265-76; Walker 2005, 400-1).

It was fascinating to observe what UK citizens found acceptable or offensive. Detention without trial and civil contingencies, together with the period during which a suspect can be held for questioning all created a political furore in the UK. This subject was revisited again under Gordon Brown in 2010 and his efforts to extend detention were defeated in the House of Lords by the recently retired

Director General of MI5 who declared his proposals to be nonsense. ID cards have also formed a perennial subject for debate. However, equally important changes affecting UK citizens that have occurred outside the UK attracted almost no attention. After uneasy negotiations, the EU and the United States came to an agreement about the sharing of airline passenger data. A similar agreement gives US counter-terrorist investigators access to data on money transfers in Europe completed via the ubiquitous Swift system. There were also moves to require European telecom providers to retain data on their callers in order to assist investigators. These decisions resulted in the creation of vast warehouses of data relating to UK citizens, which can be aggregated and shared with private entities, but which are not within national control. All this could have been read about in the specialist press, but both UK citizens and their representatives were largely obvious to the creations of this multinational transatlantic security state, until the Snowden "revelations" of July 2013 (Mathieson 2005, 1-2; Rees 2006, 231).

7.6 Iraqi WMD, Downing Street and the NSC

Non-compliance with UN resolutions on Weapons of Mass Destruction (WMD) triggered a controversial invasion and occupation of Iraq in 2003. Prior to this the UK government had decided to release two public dossiers on Iraq which it claimed to be based on intelligence material. The dossiers had been prepared for public consumption and were not actual declassified intelligence reports. Sceptical journalists could not believe that government press officers had been able to resist the temptation to enhance the dossiers. Subsequently, bitter arguments were played out in the full glare of publicity and rendered the security state more visible than ever before. In particular, the role of the Joint Intelligence Committee (JIC), a hitherto little known organism devoted to high-grade analysis, became the subject of national debate. Although the dossiers were in line with a long-term trend of allowing intelligence a more public profile, they also risked the charge that intelligence was being used to generate political support rather than to illuminate policy issues. Quality control on the dossiers, especially the second dossier, was very low.

Following the invasion, no WMD were found. The controversy intensified and there followed an unprecedented 'season of inquiry' in Whitehall and Washington, with no less than four UK investigations between July 2003 and July 2004. Intelligence on Iraqi WMD was the subject of the first inquiry by the Parliamentary Select Committee on Foreign Affairs and the second inquiry by the ISC. The third, chaired by Lord Hutton, looked into the death of Dr David Kelly, a government scientist who had been closely cross-examined by the first enquiry. Finally, Lord Butler, a former Cabinet Secretary, was called in to conduct a more general investigation into the UK WMD intelligence. The Hutton inquiry, in particular, treated academics and journalists to a remarkably detailed view of UK security state (Davies 2004, 495-520). Lord Butler's inquiry contradicted the findings of the ISC on the so called 'reliable sources' of UK intelligence on Iraq, revealing the capabilities of ISC, Parliament's standing oversight committee as weak (ISC 2003, 51; Butler 2004).

Was the Iraqi WMD episode a case of intelligence failure by the UK agencies, or deception by politicians? Inevitably, the answer is 'both'. Having badly underestimated Iraqi WMD stocks in 1991, intelligence officers did not wish to be caught out a second time and so opted for 'worst case analysis'. Moreover, the allies co-operated so closely on WMD estimates that, far from challenging each other's findings, they succumbed to a form of 'Groupthink'. Only the Dutch and the Canadians expressed serious doubts. However, there was also government dishonestly. There was some plausible intelligence to suggest that the Iraqi's might have hidden some old stocks from 1991. There was also some evidence that Iraq continued to seek WMD components on the world market and had future ambitions. However, there was no plausible evidence for the core claim that Iraq was engaged in 'continued' production of WMD. This latter assertion was made forcibly by the Prime Minister in his personal forward to the Iraqi WMD dossier (Aldrich 2005, 73-5, 81). Butler noted that there was no change in the intelligence reports on Iraqi WMD during the period 2002-3, when the UK shifted dramatically from a policy of containing Iraq to confrontation (Runciman 2004, 76-7).

There are interesting and paradoxical lessons for enhanced accountability here. These four-fold inquires into the security state deflected accountability downwards. Their remits did not allow an investigation of the relationship between intelligence and policy-making and so transparency translated into a hunt for minnows, while the big fish swam away. More importantly, many concluded that there was overall management of the burgeoning UK security state, compounded by Blair's informal style of government. At Cabinet Level there was supposedly a Ministerial Committee on the Intelligence and Security Services. Yet despite repeated exhortations, this body never met during the entire Blair administration (Davies 2013, 272-91).

Brown and Cameron both concluded that Cabinet machinery was in need of improvement and strengthening. As a result they developed the National Security Strategy and eventually the National Security Council. In the context of the latter the Prime Minister meets face to face with all three intelligence and security chiefs once a week. The intelligence chiefs have been promoted from the JIC to this new body where they interface directly with the PM. The JIC continues to review intelligence on problems while the NSC (Official) produced possible solutions to review by the main body (Davies 2013, 293-9). The NSC is widely regarded as a success, not least because it has integrated wider spectrum of Whitehall players, including those responsible for organised crime and overseas development. However, Cameron had tended to use it operationally rather than strategically. The presence of the intelligence and security agencies in this new forum has tended to drive a more interventionist and action-orientated culture (CI).

7.7. Terrorism after 2005

Attacks on Madrid in 2004 and London in 2005, together with the planned attack on airliners leaving Heathrow in 2006 revealed a massive domestic challenge. MI5 had taken an interest in radical Islamic groups in the UK during the 1990s but had not been greatly concerned about their presence. Exiles were interested in opposing their home governments in Saudi Arabia, Pakistan and Algeria, and were regarded as unproblematic from the point of view of London. However, Al Qaeda sought to mobilise these groups in a world-wide war against the United States and its allies (Gerges 2005; Bamford 2004, 739-40). Accelerated by the controversy over the Iraq War and the UK's closer association with the United States and Israel, radicalised Islamic groups suddenly became a problem. The London bombings of 7 July 2005 also underlined the scale of a new indigenous threat (Gregory & Wilkinson 2005). Western policies had energised many constituencies that would not have thought to attack the UK a decade ago. As a result, the number of active individuals were, and remain, beyond the capacity of even an expanded security state to keep under surveillance (Herrington 2015, Pythian 2006).

During 2006, Elizabeth Manningham-Buller, Director General of MI5, explained that there were 1,600 individuals of concern within the UK (Manningham-Buller 2007). Surveillance of one suspect requires the allocation of twenty operatives. Even with the expansion of MI5, larger specialist police elements, and the occasional co-option of specialist military units it has not been possible to watch more than 200 people at any given time. The Metropolitan Police Commissioner, Sir Ian Blair, revealed in the summer of 2005 that he was spending £500,000 a day over budget on terrorism-related security measures. The security state is at full stretch and this is also depleting the ability to counter organised crime and espionage (Harfield 2006, 743-61). This paved the way for greater technical surveillance.

Meanwhile harsh American tactics triggered a change in the attitude of the part of the UK judiciary. During the Cold War, commentators were inclined to observe that UK judges were cowardly when confronted with the spectre of national security rationales (Lustgarten and Leigh 1994, 321). However, following revelations about Guantanamo, Abu Graib and 'special renditions' a new climate is evident. Equipped with the Human Rights Act of 1998 senior judges have become more robust in challenging the security state. The most obvious example is torture. On 8 December 2005, the House of Lords ruled that evidence obtained under torture from third countries was inadmissible in UK courts. The subject of torture had resonance and judges gradually came to conclusion that the UK oversight committee, the ISC, was giving more attention to efficiency and effectiveness than to ethics and the law. Some have alleged that the planned multiple attacks against airliners in the UK in August 2006 were thwarted by intelligence gained after the Pakistani security authorities had vigorously interrogated Rashid Rauf, a British subject. But the extent to which intelligence derived from torture has helped to thwart plots or attacks in the UK remains unclear and will probably remain so (Danchev 2006, 587–95; Campbell and Ramesh 2006).

Government has sought avenues by which it might discourage radicalisation, but has moved uncertainly in this area. Efforts by the Foreign Office to engage directly with radicals have been dismissed as too timid by some and tantamount to appeasement by others. Institutionally, the desire for a more sophisticated approach was signalled by the creation of a new Office of Counter-terrorism and Security within the Home Office in August 2007 under Charles Farr, a diplomat with extensive experience of counter-terrorism. Simultaneously, the post of Intelligence and Security Co-ordinator in the Cabinet Office has been downgraded. Farr's new office contains a Research Information and Communications Unit headed by Jonathan Allen, another diplomat who has a background in public relations. This represents an overt drive to win hearts and minds and parallels longstanding covert information activities. The creation of a Home Office unit run by diplomats also underlines deterritorialization and the end of a security state that has a largely domestic focus.

7.8 Intercept Modernisation Programme (IMP)

The identifications of a substantial domestic threat linked to external accelerators led to a fundamental reconsideration of attitudes towards surveillance practices in the United Kingdom. Human surveillance teams were swamped and proposals were brought forward that enhance the capabilities of intelligence agencies to monitor the domestic population, which considerably blur the established boundaries between foreign and domestic intelligence activity. Traditionally, there had been relatively few limitations placed on the collection of intelligence overseas. Intelligence agencies, such as GCHQ, have been entitled to monitor the communications of foreign governments and people living abroad without much hindrance, facilitated by permissions that were wide in scope know as 8/4 warrants. The opposite can be said of the surveillance of people living within the United Kingdom. In the past, domestic monitoring has been constrained by conventions that have encouraged focused activity to prevent the widespread surveillance of the population. Most importantly, Home Secretaries were traditionally watchful of warrants against domestic targets and have rejected requests.

However, new communications technology, combined with a rising terrorist threat, led to calls for 'modernisation'. The problems associated with voice over internet were particularly worrisome, as was anticipated that over the next ten years most telephone traffic would move to the Internet. Many argued that a more technical approach would enable the intelligence agencies to passively monitor much larger numbers of people and enable them to target their scarce human surveillance teams more effectively the most dangerous individuals. Finally, as a result of high-profile terrorist attacks such as 7/7, the government has become more risk averse in its approach to surveillance.

In the last decade, the UK government has made a number of key proposals that demonstrate a clear shift towards greater surveillance of the domestic population. British ministers urged Europe to pass legislation that would require mobile phone companies and Internet service providers to retain vast amounts of records relating to personal emails, details of web pages accessed and telephone calls for ten years. This 'communications data' would be made accessible to the police and intelligence services on request. The proposals were denounced by privacy campaigners as one of the most wide-ranging extensions of government security surveillance over private individuals ever contemplated. The main opponent was in fact the Internet industry itself, who resisted the plans vehemently, again stressing issues of privacy and business confidentiality. The material in question here is not the content of the call or communication, but the names and addresses of customers, the source and destination of their emails and the addresses of web sites visited. In 2006, this measure finally passed into European law (Mathieson 2005).

This mass retention of data by ISPs did not go far enough for the UK. In 2008 the British government unveiled a new domestic intercept plan of unprecedented proportions. The Home Secretary Jacqui Smith announced the British government's remarkable Intercept Modernisation Programme (IMP). Costing an estimated £12 billion pounds, this project amounted to a vast surveillance concept that was quite beyond the bounds of anything previously been seen in the United Kingdom. Despite the fact that Europe had finally agreed to compel ISPs to retain everyone's past communications data within their own companies, the UK nevertheless proposed to build a vast government-run silo to duplicate essentially the same function. Simply put, the government wished to hold all the data itself. This would entail the recording and storing the details of every telephone call, email, text and instance of web access by each person in the UK, Lord Carlisle of Berriew, QC, the UK's Independent Reviewer of Terrorism Legislation (IRTL) immediately expressed anxiety about the new government-run database, asserting that: 'As a raw idea it is awful'. He added that it would lead to the authorities undertaking searches 'willy-nilly' and without review (Verkaik and Morris 2008).

In late 2008, growing public hostility to IMP prompted the government to withdraw the bill at the last minute. Instead, government has resolved to advance the plan by stealth. Remarkably, and without any legislation, a pilot scheme at an estimated cost of £2 billion pounds was launched. Indeed, sample 'probes' were established at the facilities of one major fixed line telecom operator and one major mobile phone provider. The British government had always insisted that IMP was merely about maintaining an existing and traditional capability to do interception in a world of rapidly changing technology. However, the reality looked rather different. In April 2009, GCHQ advertised for new senior staff to direct an ambitious programme which it called 'Mastering the Internet'. The sinister title of this project caused alarm and GCHQ was soon forced to issue a public statement denying that it was developing technology to enable the monitoring of all Internet use and phone calls, or to target everyone in the UK.

However, in August 2009, government denials that it had ambitions for expanded surveillance met a direct challenge. Britain's own telecommunications firms and ISPs, including British Telecom and Virgin, condemned these plans as an unwarranted intrusion into people's privacy. The very companies that the British government was depending upon to help it to implement the scheme asserted strongly that government officials were not being honest with the public about the vast scale of monitoring that they were planning. It told the government that: 'We view the description of the government's proposals as 'maintaining' the capability as disingenuous: the volume of data the government now proposes [we] should collect and retain will be unprecedented, as is the overall level of intrusion into the privacy of citizenry … This is a purely political description that serves to win consent by hiding the extent of the proposed extension of powers for the state.' The UK's ISPs also boggled at the mammoth scale of the private information they were being asked to retain themselves on the telephone and internet use of British citizens. Indeed, they complained that they were 'not aware of any existing equipment' that even would enable them to 'acquire and retain such a wide range of data' (Leppard 2009).

What did government want with all this detail? And why did they want to hold it in one place? The answer is quite simply 'data-mining', a practice which now constitutes the most insidious threat to personal liberty. What makes surveillance different in the age of ubiquitous computing and the mobile phone is that our data is never thrown away. Machines routinely store millions of details about our everyday lives and, at some distant point in the future, this can be brought together and searched in the hope of finding patterns. Devices which were introduced to make life more convenient, such as the mobile phone, are also generating a detailed electronic narrative of our lives. In 2009, the British public sent 60 billion text messages, a microscopic account of our personal interactions. A decade ago, such data was discarded by many companies, but with the cost of warehousing data halving every two years – many now choose to retain it. What many governments now wish to do is take this data over and use it to produce a wholly new kind of intelligence with new powerful forms of analysis that no-one anticipated five years ago (Sommer and Hosein 2009).

Data-mining is the use of computers to comb through unimaginable amounts of information looking for patterns and statistical relationships. It allows governments to search for individuals or groups of people with particular types of behaviour and to profile them as suspicious. Data-mining is as powerful as it is dangerous. It is powerful, because it allows the sifting of titanic amounts of private information, and it is dangerous because it often throws up 'false positives'. In other words, some people will look suspicious because a number of chance activities have coalesced to generate something which a computer thinks is a problem. It also permits social profiling. At present, data-mining is limited because government can only access so much information. However, the appetite is clearly there. Under the Regulation of Investigatory Powers Act 2000 (RIPA), the authorities can go to ISPs or mobile phone companies and ask them to hand over details of customer phone, email and internet habits of specific individuals without seeking a warrant. A staggering 504,073 requests were made by the authorities in 2008. Although this is too many requests, it is still 'retail surveillance' because it relates to individual persons. Data-mining is the next step and means wholesale surveillance. For the state, vast reservoirs of person data such as Facebook and Google are now the great prize and Snowden suggests that both NSA and GCHQ had accessed them (Harding 2013).

7.9. Snowden

In the late 1990s, NSA was in crisis. The Internet was expanding exponentially and volume of mobile phone usage had gone off the scale. The information and communications revolution was in full swing and yet the budget of NSA and its British partner had been cut. Michael Hayden, Director of NSA, sought to develop a closer relationship with Microsoft and Google in order to try to stay ahead of the wave. He also privatised many of the NSA's back office services in an effort to cut costs and harness the dynamism of the global computer industry. In through this back door stepped Edward Snowden. By 2012, Snowden had moved to a new NSA job, this time in Hawaii, a key nodal point in the worldwide listening chain run by NSA, GCHQ, and its allies. It gave him access to thousands of documents showing how the West undertook top secret signals intelligence in the twitter age (Harding 2013, 37-49).

On 6 June 2013, *Guardian* journalist Glenn Greenwald revealed that the NSA routinely collected the telephone records of millions of Verizon customers. Top American academic lawyers at Harvard and Yale judged to be illegal and unconstitutional activities. Details followed of another top secret operation known as PRISM in which the NSA accessed systems owned by internet giants such as Facebook, Yahoo, Microsoft and Skype. President Obama sought to soothe public concerns. However, it soon became clear that Snowden had stolen far more than documents relating to one or two mass surveillance programmes and many concerned UK activities. Publicly the American government were robust in defending their programmes, privately they were aghast at having revealed the parallel activities of their partner British agency, GCHQ.

Newspapers soon revealed how Gordon Brown had authorised GCHQ to bug foreign leaders at two G20 meetings in London in 2009. The timing of this story was uncomfortable, for Cameron was about to host a G8 summit in Northern Ireland. Vladimir Putin, Barak Obama, and Angela Merkel were all present. Snowden's revelations raised an obvious question: what had the Prime Minister authorised GCHQ to do against his professed friends with whom he was now sharing the podium? The media loved the sense of personal animosity and every newspaper carried a photograph of an anxious Merkel talking on her ever present mobile phone (Aldrich and Cormac 2016).

The government was not slow to respond. In July 2013, two men from GCHQ – nicknamed "the Hobbits" by the newspaper's journalists – arrived to discuss destruction of the Guardian's hard drives. On 20 July they returned with a degausser to destroy magnetic fields and headed down to a stuffy windowless basement deep beneath the *Guardian*'s offices. *Guardian* staff watched as the hobbits took drills and angle-grinders to the hardware. Sparks flew. What Cameron was trying to cover up was that he had looked at prosecution under the Official Secrets Act and backed away from the option of trying to jail the editor of a leading newspaper. Alan Rusbridger, the editor, had second guessed Cameron's thinking and had realised he was effectively bullet-proof.

There were three wider security issues: first, the general impact of Snowden's revelations on the communications practices of both transnational criminals and terrorists. In the short term they stayed away from their electronic devices, in the long term they sought better encryption. Second, countries as diverse as Kyrgyzstan and Brazil now realised fully the new opportunities that electronic surveillance technology offered for spying on their citizens and began queuing up to buy monitoring equipment from enterprising software firms. Third, the techniques that NSA and GCHQ had used for passive espionage opened the eyes of other states and non-state actors to their active possibilities: these could also be used for crime or sabotage. All this was not perhaps Snowden's original intention.

The UK Cabinet failed to appreciate the complexity of the problem. As NSA and GCHQ had shifted their focus from states to problematic people, and spying now depended upon supermarket loyalty cards as much as secret services, it was no longer possible to have a serious public debate about civil liberties without giving away some information about sources and methods that was useful to terrorists. Snowden was therefore, at one and the same time, hero and villain. Moreover, Cameron and his Foreign Secretary were wrong in their assertions that GCHQ had done nothing unlawful. After complex inquiries that took over a year, the Investigatory Powers Tribunal declared that GCHQ's joint programme on mass data conducted with the Americans had indeed been illegal (Bowcott 2015).

Former GCHQ officials insist that the transgression was not deliberate and point to the numbers of trained lawyers on GCHQ's staff – some of the most important people in this vast curvilinear building. They also insist that mass access to personal data was not the same as mass surveillance. In any case, much of the interest by the security agencies was in geographical data or call patterns and social networks – not call content. A great deal of this work was conducted anonymously by computers and no spies were watching citizens. By contrast Snowden, the *Guardian* and civil liberties groups found the artificial intelligence aspect of the story, with its overtones of "Terminator", the most frightening. What actually constituted intrusive surveillance was now up for debate – and very much in the eye of the beholder (CI).

On of GCHQ's main failings was that they had simply refused to explain themselves. While MI5 and MI6 had recently opted to open their archives to independent historians, GCHQ refused to go down this path. Even their American equivalent, the NSA, had declassified a formerly Top Secret "Codeword" four volume history running to 1989. GCHQ's press office was a mess with one of their press officers, Alfred Bacchus, trying to sue them for racial discrimination. Former Directors of GCHQ like David Omand joined the debate in the summer of 2013 and made important contributions, but GCHQ itself was conspicuous by its absence. Cameron stepped in and made a dramatic gesture. He appointed Robert Hannigan as the new director of GCHQ, someone who had never previously worked in an intelligence agency. Hannigan had begun his career in a public relations firm, before joining the press team at the Northern Ireland Office. Promoted rapidly after his boss left to join Alastair Campbell's unit at Downing Street, his main expertise was in communications. Cameron also created a new press section within the central intelligence machinery in Downing Street to begin the fight back against what he saw as a group of determinedly anti-intelligence journalists, NGOs and lawyers.

8.The Oversight of Intelligence and Security Agencies.

8.1 Oversight and the European Court

In the 1990s, the UK security state faced nothing short of a regulatory revolution. The main driver was two cases in the European Court of Human Rights. The first was brought by in 1984 Harriet Harman when an MI5 officer revealed that files were held on her and a colleague. The nub of their argument was that MI5 had no legal standing and therefore lacked proper mechanisms for oversight and accountability. In the subsequent Leander Case of 1987, the European Court found against the Swedish security service on similar grounds. Like most European states, the UK and Sweden had dealt with its security services by pretending that they did not exist and hoping that its operatives were never caught. Across Europe, states now rushed to put their agencies on the statute books. Despite initial anxiety, a firm legal status and clear guidelines for surveillance have meant that agencies are free to carry out more operations. The legislation has been permissive since the criterion is now 'is it legal?' rather than 'will we get caught'? This outcome was not anticipated, nor indeed welcomed, by civil rights campaigners who had long advocated greater regulation.

The Security Service Act of 1989 and the Intelligence Services Act of 1994 placed the UK's three main agencies on the statute book and gave them formal and open remits. Additionally, the functions of the National Criminal Intelligence Service (now National Crime Agency) were covered by the 1997 Police Act. MI5 retained a limited brief for countering subversion, including far right organisations, although the problematic term 'subversion' was no longer employed in the statute. A range of tribunals and commissioners, normally former judges, were created to deal with public complaints arising from operations. The security services introduced staff counsellors to respond to colleagues who had anxieties about their work. Most importantly perhaps, they also conjured into existence what has become the most visible mechanism for UK accountability, the Intelligence and Security Committee.

The UK Intelligence and Security Committee (ISC) outwardly resembled a Parliamentary Select Committee. However, it was created as a statutory committee and has not enjoyed the full powers of a select committee, nor was it owned by Parliament. Until recently its members were selected from Parliament by the Prime Minister only and reported to him. ISC reports are made public, together with the responses of government, but in a sanitised form and can be edited by the Prime Minister. In short it was a committee of parliamentarians but it was not of Parliament. Despite recent reforms that bring it closer to Parliament, the ISC still lacks a sizeable and serious research component, rendering it anodyne by comparison with its foreign equivalents. Meanwhile members of genuine UK Parliamentary Select Committees, typically on Home Affairs, have argued that the creation of ISC curtails their own right to introspect into the security agencies. Some have complained that its reports are mere 'audits' and contain only limited reflection or analysis, albeit there is a good working relationship with the agencies. There is little consensus in academia or the press on the effectiveness of the ISC.

In theory, the ISC sets its own agenda, although in practice it does feel inclined to respond to issues raised by the media often in tandem with campaign groups. It publishes annual reports in a redacted form and has also produced a number of special reports on subjects it considers important. The Chair of the ISC also appears in the media with increasing frequency. The ISC mandate is limited to the consideration of matters such as administration, policy and expenditure, nevertheless the ISC has grown in confidence over the years. It has increasingly reviewed operational matters and some have suggested that it has become a serious critic of the agencies, typically in examining the handling of detainees in Afghanistan and Iraq (Gill and Phythian 2006; Phythian 2007).

In July 2007, Gordon Brown's Green Paper on 'The Governance of Britain' undertook to consult on how the ISC could be brought 'as far as possible' into line with that of other select committees, including the restoration of the investigator whose services were abruptly dispensed with in 2004. Similar notions were aired in the 2008 UK National Security Strategy. In 2013, the Justice and Security Act 2013 reformed the ISC, making it a Committee of Parliament, providing greater powers; and increasing its remit, including oversight of operational activity and the wider intelligence and security activities of Government. Beyond the three intelligence and security Agencies, the ISC now examines the intelligence-related work of the Cabinet Office including: the JIC; the Assessments Staff; and the National Security Secretariat. It also provides oversight of Defence Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism in the Home Office. The Security and Justice Act of 2013 also sought to shore up the ISC’s position as the main focus of formal oversight, fending off the efforts of judges and courts to encroach on this role. Although reforms included in the 2013 Justice and Security Act gave Parliament the power to approve its membership, members must still be nominated by the Prime Minister in consultation with Opposition leaders.

Historically, it has often been asserted that the Intelligence and Security Committee (ISC) differs from other parliamentary committees in that it is more secure and does not leak. Working ‘within the ring of secrecy’, they enjoy considerable access to classified documents and intelligence personnel. The agencies set great store by the protocols of secrecy and its approach to sensitive information has been central to building a relationship of trust. Many of those chose to serve on the committee are former ministers and are often chosen for their sober demeanour. However, recently the Chair of the ISC found it necessary to resign over a parliamentary ethics issue and one of the ISC's reports appears to have been leaked to the *Sunday Times*.

More broadly, academic commentators and campaign groups are also in two minds about the UK's modernised security state and its developing oversight mechanisms. Some have seen this as genuine cultural change while other have argued that the advent of tribunals, commissioners and counsellors was in part an attempt to keep disaffected intelligence officers away from the unpredictable realm of courts and normal employment tribunals. Very few complaints made to any tribunal concerning intelligence and security matters have been upheld since their creation in the mid-1980s. Depending on one's view, this is either rather reassuring or else rather worrying (Brown HC 314 2007, sec.38).

The argument that reform and modernisation has in reality meant greater opaqueness is most compelling with regard to revised Official Secrets Act. The revised act removed the notorious catch-all Section 2, replacing it with offences that related to specific groups of people and information. However, the new act also went to great lengths to remove the possibility of a 'public interest' defence to prevent 'whistle-blowers' using the courts to air their views about abuses within the agencies. Subsequently, 'whistle-blowers' such as David Shayler, the dissident MI5 officer, have had tried to fall back on the ECHR Article 10 with its protection of freedom of expression. Notwithstanding this, 'whistle-blowers' have continued to trump government lawyers, as underlined by the Catherine Gun case in 2005 and the Derek Pasquill case in 2007 (Gill 1996, 313-320; Morrison 2008, 51-2).

Within the UK Parliament, the ISC has had to contend with more serious rivals. Several parliamentary select committees have remits that overlap including those on Defence, Foreign policy, Home Affairs, Northern Ireland and Terrorism. Some have even been inclined sought to carry out their own investigations in areas also scrutinised by the ISC, an example being the Foreign Affairs Committee's inquiry into the government's presentation of the case for war in Iraq (FAC 2004). The Joint Committee on Human Rights has also looked at allegations that UK intelligence personnel were complicit in torture (JCHR 2009). The appointment of an independent committee chaired by Lord Butler to examine intelligence on Iraqi weapons of mass destruction in 2004 was widely seen as conceding that the ISC lacks enough traction to deal with serious problems (ISC 2004, Butler 2004).

Most academic observers are now rather sceptical of the speedy reassurance offered by the ISC in July 2013 in the wake of the Snowden revelations. In particular, the reception of various materials without a warrant from the NSA appears to contradict assurances by the ISC that where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already available. The extent to which all material received by GCHQ from its overseas partners is covered by warrants is still unclear. According to the evidence provided by GCHQ to Investigatory Powers Tribunal, beyond intercepted material which is received under a RIPA warrant, Cheltenham also receives a complex range of unanalysed material without a relevant interception warrant when 'it is not technically feasible to obtain the communications via RIPA interception' (Ogilvie & Sankey, 2014).

The intelligence and security services usually request warrants of two different kinds under the Regulation of Investigatory Powers Act 2000. Home Secretaries can approve a warrant under section 8(1) that focuses on the interception of communications in relation to specific persons or premises. Foreign Secretaries can approve warrants under section 8(4) which apply to external communications and are often more general in scope. Both warrants can apply to material gained by working with other countries. The debate has focused on further unanalysed intercepted material that was received without the need for a warrant signed by the Secretary of State. Both the

Secretary of State for Foreign Affairs and the ISC had quickly cleared GCHQ in relation to the PRISM allegations, partly on the basis that GCHQ had insisted that it had done nothing unlawful. (As yet few have asked about further material received from other Five Eyes partners, members of the Nine Eyes system in Europe like France or other important bilateral partners like Sweden.) The ISC now been shown to be off the mark on the matter of Snowden, as it was over the quality of intelligence and Iraq in 2004 and so its ability to introspect into these matters is now in doubt.

8.2 Role of the media

The mistakes of Parliament and Cabinet Ministers highlight the growing importance of the press as an additional mechanism of oversight and accountability. As the House Commons Home Affairs select committee has recognised, press freedom was central to the exposure of the Snowden affair. In the UK, press freedom is guaranteed by the ECHR provisions on freedom of expression rather than a US type First Amendment. Ewan MacAskill, one of the key UK journalists covering the Snowden affair claims that whereas US has been free to report the Snowden documents, *the Guardian* came under repeated pressure from the British government to stop. This comparison is not entirely correct. In the United States a more chaotic system has prevailed with direct telephone negotiation between government and editors, which amounts to a less formal and less effective version of the UK system. It is also not quite correct to say the United States does not have an equivalent of the Official Secrets Act. In fact the US has legislation protecting both intelligence identities and also special information relating to sigint, albeit the latter is rarely deployed against the press (MacAskill in Moore 2014).

Like the US Government, the UK Government rarely takes direct legal action against the press over the leaking of secrets in the UK. This is partly because ministers and former ministers together with their aides are often the source of leaks, moreover when they address previously secret matters in their own memoirs they are seemingly immune form any retribution. Law officers are also aware that there is a very real danger the jury would acquit on general principle. Nevertheless, during the Snowden affair, the UK government threatened injunctions. The most bizarre episode was the destruction of hard drives in the basement of the Guardian from the computers used to store the Snowden documents under supervision by GCHQ (see above p.22). As a result, the *Guardian* no longer keep copies of documents in London or New York and is reliant on the *New York Times* for access to research material. Guardian journalists now work on the Snowden case by visiting *The New York Times* office to read the documents. Some have argued that Snowden case shows that proper intelligence oversight could only be achieved if the UK adopted something similar to the First Amendment. However this seems to ignore the fact that the reports of Dana Priest over secret prisons in Europe were censored in 2005 at the request of the US government – removing the names of the counties were the prisons were located. In short, the UK and US systems are closer than they appear at first glance.

The core of the UK system for moderating the conflicting imperatives of national security and public interest reporting is therefore a fundamental part of the wider ecology of intelligence oversight. Something known as the Defence and Security Media Advisory (DSMA) system, previously DA-Notice system, allows for the voluntary redaction of sensitive national security material. This system encourages informal consultation between editors and government officials before a story is published and seeks middle way, permitting many stories to be published but often with particular details removed. The initial decision of the *Guardian* to disregard this system when covering the material revealed by Edward Snowden intensified a pre-existing debate about whether the DSMA System could function effectively in ‘the age of the internet and worldwide social media’.

The UK government's primary argument for media restriction is based on its international responsibilities a continued major role that the UK plays in world affairs. Military and intelligence operations in support of this mean that press reporting can pose risks to UK personnel at home and abroad and might cost lives or compromise military operations. Although news is international, most of the UK national security press stories have a domestic origin and so the DSMA System continues to exercise traction over the majority of stories that might damage national security. The DSMA system is entirely voluntary and this limits its power to influence the media. However, press consultation and the inevitable conversations with the agencies allows the option of injunction under OSA and also potentially the gathering of intelligence against leakers during extended conversations that might then be leveraged thought other channels (Vallance in Moore 2015).

How far has the guidance of the DSMA System been responsible for shaping the extent to which Snowden was cover in the wider UK media? There are certainly standing DSMA notices covering matters such as signals intelligence and discouraging its discussion. The response in the UK broadcast media has been uneven, while other media outlets largely tended to ignore the Snowden revelations beyond the summer of 2013. The BBC has been episodic in its discussion of the matter while coverage by the *Times, Telegraph, Mail* and others has been very limited. But journalists suggest that this is less because of DSMA guidance and more because the Murdoch papers did not wish to give extra air time to a *Guardian* story which some felt had become a crusade. In some cases the content was simply judged too technical even for the broadsheet newspapers (CI). National culture is a factor here too. In the US, citizens are inherently suspicious of federal government. In Germany, the Snowden revelations evoked memories of the GDR security apparatus. But in the UK, electronic surveillance is associated with the more benign narrative of Bletchley Park - or even James Bond (MacAskill in Moore 2014).

There are now difficult tensions between official secrecy and accountability. Current intelligence priorities are less about Russian submarines or Chinese missiles; instead they are more about people. Accordingly it is now more difficult to have a detailed discussion about civil liberties and personal freedoms without exposing information which endangers national security. In the UK, action under the OSA is a matter for the Crown Prosecutors who move through two stages when deciding is it worth launching a prosecution. The two tests are discussion about the strength of the evidence and then the public interest. In the Snowden case there was strong evidence that the OSA had been deliberately broken and a so prosecution could have been undertaken. But would a prosecution have been in the public interest? (McDonald in Moore 2014) While government insists that OSA prosecutions are purely a matter for law officers, past history suggests that these decision are in part political, especial the decision to drop failing or embarrassing legal actions (Aldrich 2010, 360).

8.3 Oversight and International Intelligence Co-operation

In the UK, the Snowden affair has shone a bright light on the problem of oversight and international intelligence co-operation. Such co-operation - or 'liaison' - has long been identified as an area that is opaque to oversight and accountability bodies, indeed it also constitutes a notoriously difficult area for academics, journalists and other researchers. This is partly because of the extreme secrecy that intelligence agencies attach to 'liaison' . Not only do countries wish to avoid damaging these relationships but also they are not always keen to inform their own political masters of their degree of dependency on friends for certain streams of intelligence. Moreover, intelligence co-operation is a diffuse activity and so intrinsically hard to monitor. Although some larger intelligence agencies boast an office that manages liaisons, in reality it is spread across every aspect of the intelligence process (Alexander 1998).

For more than a decade the 'black hole' of international intelligence co-operation has been expanding rapidly. Stephen Lander, the former Director General of MI5, has observed that the exponential increase in international intelligence co-operation constitutes the most significant change within the world of intelligence since the 1990s (Lander 2004). Most obviously, since 2001, the 'Global War on Terror' has greatly accelerated the scope and scale of international co-operation. It has also prompted more aggressive operations by clandestine agencies - including rendition - which some legislatures have been keen to investigate. This reflects a more fundamental change in the style intelligence activity that has been underway since the mid-1990s, namely Globalisation (see above 7.5). Most of the targets that intelligence agencies have been asked to address since the end of the Cold War have an increasingly globalized dimension - and in response - intelligence and security agencies are being forced to globalize their activities. Agencies, together with their operations and their targets are moving apace down the transnational trail. The resulting changes include the development of a global world of domestic security liaison and accelerating privatisation of some key functions. Unsurprisingly, accountability and oversight have been left behind.

'Globalization' is a word that social scientists use *ad nauseam*, but rarely pause to define. Jan Arte Scholte, in his widely referenced text, has tended to emphasise the spatial (or spatio-temporal) aspects of this phenomenon. This perspective is primarily about social and political geography, distinguished by the development of 'supraterritorial spaces', which exist awkwardly alongside conventional sovereign territoriality (Scholte 2000). This particular notion of globalization speaks directly to current intelligence targets, agencies and their operations. Since the end of the Cold War, states have been increasingly confronted by security problems that emanate from non-state actors. States have made things worse by deliberately opening up their borders to free flows of money, expertise, communications and ideas in order to benefit from exponential increases in volumes of trade. Terrorists, warlords and criminals have been quick to capitalise on this fluidity. Many of these adversaries have ridden the wave of globalization, employing dispersed networks to hide their activities and achieving a somewhat mercurial existence (Naim 2005).

We are not only seeing a quantitative increase in co-operation between the intelligence services of different states, but also qualitative changes. We are seeing improbable intelligence partners, rather than the familiar combination of Cold War intelligence collaborators. While the majority of meaningful intelligence exchange remains bilateral, multilateral co-operation in areas such as training and field operations is also growing. Moreover, we are witnessing a remarkable growth in operations. The extent to which all these bilateral relationships and exchanges are adequately governed by legal agreements is open to doubt (CI).

Globalization has been closely associated with the cosmopolitan idea of global citizenship, implying a common ownership of liberal and humane values - and of course - human rights. Certainly the institutions of the European Union, are now taking a stronger interest in intelligence oversight. Arguably they have little choice given the growing profile of intelligence as a mode of policing the underside of globalization. The European inquiries into rendition were notably successful and helped to prompt important research on this subject by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) in co-operation with the Norwegian Parliament (Born & Leigh 2010).

The main change in terms of oversight has been the rise of global civil society. Here, globalization manifests itself the inter-connections between domestic police and security services, eroding the distinction between what constitutes domestic and foreign. Finally, private security companies and corporate providers of national infrastructure - sometimes themselves multinationals - are playing a larger part in intelligence in the form of citizen groups and transnational bodies that campaign on thematic issues, such as human rights and the environment. The number of transnational NGOs broadly doubled in the 1990s. Of course, transnational civil society contains both civil and uncivil elements. The facilitating aspects of globalization - not least the internet - that make new forms of oppositional politics possible are often the same aspects that have encouraged new forms of insecurity from transnational threats. Some would argue that this informal network of counter-surveillance by activists and pressure groups, although unable to call intelligence agencies directly to account, has nevertheless proved to be less troubled by state boundaries than national committees and commissions of inquiry (Kalathil and Boas 2003).

If we accept that intelligence activities are now globalizing, there is an obvious mismatch between the emerging new style of operational activity and the traditional patterns of accountability which look increasingly parochial. Intelligence co-operation or 'liaison' has always presented a challenge for bodies charged with accountability and oversight. However Snowden has demonstrated that the scope and scale of co-operation has resulted in a qualitative change that now renders traditional forms of accountability - rooted in the sovereign nation-state - increasingly outmoded and incomplete.

The main driver of this informal civil society has been the press working with campaign groups. But what might nation states themselves do to extend national accountability to encompass intelligence liaison? The likelihood of committees of politicians being allowed to peer into this sensitive area remains low. However, a little explored alternative would be Inspectors-General with extended authority to operate in more than one country. If states co-operating on intelligence can agree on complex protocols for the distribution of sensitive material, they can agree on common guidelines for investigating officers. Inspectors-General have obvious short-comings in the sense that their inquiries are internal, operating rather like police internal affairs units. Yet arguably, in the ultra-secret world of intelligence co-operation, this is possibly what is required. A senior intelligence official, perhaps the respected former head of a national service, could serve as a roving Inspector General for a number of allied countries working together, perhaps reporting to a body such as NATO. This would doubtless horrify many officials, but it has been actively discussed by government lawyers as conceivable, at least in the context of the more prominent US, EU and Commonwealth services.

9.The Protection of Privacy and Civil liberties in the UK

9.1 The limited role of the ISC

Many UK MPs are somewhat ill-informed about intelligence and especially about the technical issues around interception. This is disturbing given that GCHQ's response when challenged by its own staff on a particular programme is often to assert that they have done nothing unlawful. At first glance this formulation seems reassuring, but it is clear that parliamentarians themselves had little idea of the nature and range of the powers that they had extended to GCHQ and others under legislation like RIPA. Some in Westminster clearly believe that the primary role of parliamentary oversight is to focus on human rights issues. This is particularly true of members of the House of Lords. Some have emphasised the importance of Parliament in ensuring that the intelligence services do not break any international obligations, notably those covered by the ECHR. This has been an area of concern since 2005 with the controversy around extraordinary rendition and Dana Priest's exposure of secret prisons in Europe (Bochel et al 2014, 163). Former Cabinet Minsters have publicly expressed anxiety about the imbalance of intelligence exchange between the UK and the US, wondering aloud about the 'errands we perform in return' to counterbalance this inequality (Patten 2005, 97).

As we have seen, the ISC's remit is not focused on defending civil liberties and is instead concerned with efficiency and effectiveness. The primary defensive screen for civil liberties are firstly lawyers in the agencies themselves who are concerned that their staff do not end up in court. The secondary screen consists of judges, either in UK courts, the European court, or the Investigatory Powers Tribunal (see below). Judges have become increasingly radical in intelligence matters, having noticed to their dismay that ISC is not much interested in rights and liberties. Accordingly, in 2013 the UK Parliament introduced new legislation which simultaneously improved the standing of the ISC but reduced the freedom of manoeuvre for courts in the UK in intelligence matters. This was a response to the decision of the UK courts during 2008-10 to make American classified documents public relating to the controversy over torture to the dismay of the UK Foreign Secretary.

ISC has nevertheless expressed the view that the law on interception needs tightening. In March 2015, the ISC asserted that a new, single Act of Parliament should replace the current complex and outdated legislation dealing with the intrusive capabilities of the UK intelligence and security agencies. Hitherto, the ISC has avoided even acknowledging some of the bulk interception activities undertaken by the UK agencies. Echoing the IPT, they have now suggested that the legal framework is opaque and obsolescent. The Labour MP Hazel Blears, a member of ISC explained their findings and emphasised the growing public expectation of openness and transparency in terms of what the agencies could were broadly empowered to do. There was also an emphasis on improving public understanding, confidence and trust.

In their latest report, the ISC have particular attention to Bulk Personal Datasets. The ISC still focuses on efficiency and effectiveness arguing that that GCHQ needed to access to internet traffic through bulk interception and insisting that GCHQ does not conduct 'blanket surveillance, nor does it equate to indiscriminate surveillance or indiscriminating surveillance. In terms of new legation that ISC have suggested that applications for warrants should be standardised. In other words, GCHQ and the SIS would need to give more detail in their 8/4 requests to the Foreign Secretary for overseas surveillance warrants, mirroring the process that MI5 currently employs. Within Whitehall the agencies would also be required to offer more detail in support of interception requests. ISC were keen to see less "thematic warrants", which are target a wider defined group and risk general collection on a large scale. They hoped that new legislations would permit shorter timescales. However, these are changes at the margin and have failed to convince the public groups with an interest in this area (CI).

Organisations like the "The Open Rights Group" have called for the Parliamentary oversight mechanisms themselves to be overhauled to provide more attention to civil liberties. They have argued that the ISC needs to be totally independent, fully accountable to Parliament and capable of offering the requisite technical, legal and ethical expertise to properly assess surveillance. But this is to misunderstand the fundamental problem of the ISC which would still suffer from something close to a conflict of interest. It would perhaps better to accept that the ISC is primarily seeking to conduct an effectiveness audit, leaving issues of right and liberties to other bodies.

By contrast, David Anderson, *Independent Reviewer of Terrorism Legislation (IPT),* has little time for the ISC and instead emphasises the importance of a replacing ministerial warrants with a US style surveillance court offering independent judgment on applications for warrants. The more astute campaign organisations have followed suite, ignoring political oversight and focused on legal challenge. They have also shifted the debate on liberties away from issue of privacy toward freedom of expression, something which enjoys more robust defence under the European Charter. This is likely to be a major battleground over the next decade.

9.2 Independent Reviewer of Terrorism Legislation (IRTL)

Oddly, one of the most effective institutions relating to matters of civil liberties, intelligence and surveillance has no standing in legislation relating directly to intelligence. The IRTL is required to report annually to Parliament on the operation of the Terrorism Act 2000 and may also comment on subsequent legislation related to terrorism. Other inquiries may be mounted at the request of the Government or on the Independent Reviewer's own initiative. “A Question of Trust", a major report on the future of investigatory powers, was commissioned by Parliament in July 2014 and published in June 2015. The essence of this role is full access combined with independence and judicial experience. Since 2001, the post has been held by Lord Carlile of Berriew C.B.E. Q.C. and then David Anderson Q.C. since February 2011 (Anderson 2014). Information gathered by the IRTL, and policy suggestions made by the IRTL are taken very seriously by the executive (Walker 2014, 4).

Comparing the work of the IRTL with that of the ISC again highlights the inadequacy of the latter. Anderson report was more through, more revealing and his proposal for change were more substantial. On the core issues of RIPA, Anderson observed:

> RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable. (IRTL 2015)

In style, but not in structure or authority, the IRTL looks most like an Inspector General. The IRTL in the UK and Inspectors General in the US and Australia have produced some of the most detailed, fair-minded and balanced commentary in an area which is highly contested and often attracts emotive language and impractical suggestions for reform. Anderson’s observations, offered in detail and at length at thought to have shaped the current governments thing on the reform of interception legislation. His main recommendation is that all warrants should be judicially authorised by a Judicial Commissioner working through a new body: the Independent Surveillance and Intelligence Commission. However the US model is by no means perfect, since the US equivalent has rarely rejected requests and was still circumvented by the Bush administration in its quest for large scale call data.

9.3 RIPA and the Investigatory Powers Tribunal

Fundamentally, civil liberties and freedom from unnecessary surveillance in the UK are limited by the historical nature of common law which emphasises protection of property rather than privacy. Privacy is a rather existential thing and UK common law does not deal with such ephemeral subjects very well. Typically, illegal clandestine searches by state officers are illegal not because of a breach of privacy but because of trespass and interference with private property. Electronic interception has not interfered much with private property and was therefore poorly regulated by UK law until the advent ECHR.

ECHR, which was gradual embraced by UK law, has given more protection to privacy. During the 1980s it became clear that tapping of telephones was a violation of ECHR article 8 – the right to privacy – if there was no proper process to authorise this. The core of the European court rulings in the 1980s was that if the state was going to undertake secret activities then there had to be legislation to authorise this and the agencies themselves needed a legal identity so that people could have a focus for an appeal against unfair treatment. In the 1990s, European secret services appeared the statute books. In the UK, these laws require the secret services to limit their activities to the purposes of national security, economic well-being of the UK, or preventing serious crime.

As we have seen, the Regulation of Investigatory Powers Act of 2000 (RIPA) has been given a hard time by academic commentators, by campaign groups and also by David Anderson as IRTL. Yet it has performed rather better than legislation in other area. Although over-complex and now outdated, it was a major step forward in controlling the use of covert human sources, instructive physical surveillance and entry to property, agents, informants and undercover officers by all UK authorities. The creators of RIPA made a commendable and visible effort to incorporate of parts of ECHR into its operating principles. The admirable ideas of proportionally and least harm were at its core and managers were obliged to show that surveillance was necessary to avoid wider public harm. It was also essential to show that the intelligence could not be obtained by less intrusive means. The rights of agents themselves also received much needed attention for the first time.

More importantly, RIPA accelerated cultural change. Together with the legislation that gave the intelligence security agencies a legal identity and framework, it has revised the outlook of senior managers. On 31 October 2001, MPs from UK Parliament's Home Affairs Select Committee visited to the headquarters of the MI5 at Thames House to discuss new proposed anti-terrorism legislation. They were received by Stephen Lander, the Director-General of MI5, who astounded them with his familiarity with the pertinent legal frameworks. The committee clerk observed: 'Did you ever dream you might hear a director general of the security service banding around articles of the European Charter of Human Rights with such fluency?' (Mullin 2003, 234).

As we have seen, RIPA also created an Investigatory Powers Tribunal (IPT) which superseded the Security Service Tribunal, the Intelligence Services Tribunal and the Interception Tribunal that had been established between 1985 and 1994. Although the IPT is a notably secretive body whose activities are hard to follow, it is potent, enjoying the power to quash warrants, destroy records and award compensation. Importantly, the tribunal can also hear proceedings brought under Section 7 of the Human Rights Act of 1998 against any of the agencies. The Human Rights Act 1998 also acts as a constraint on the agencies, but that lack of transparency by the IPT in terms of its actions is again problematic. The IPT itself finds the interactions between the various pieces of pertinent legislation complicated, and almost impossible for the public to understand.

One of the important facts revealed by the reports of the various commissioners was just how many government departments were now empowered to use covert surveillance. This included not only the obvious praetorian elements, but all departments of state and even local government. In 2008, Britain's interception of communications commissioner revealed that nearly 800 public bodies, including NHS trusts, were making an average of nearly 1,000 requests a day for communications data, including actual phone taps, mobile phone records, email or web search histories, not to mention old-fashioned snail mail. Empowered bodies also included 474 local councils who made 1,700 requests to access mobile phone records and other private information in the last nine months of 2006. Therefore, while Europe has initiated the UK security state into the new culture of regulation, this was of a facilitating kind (Garton Ash 2008).

Responding to persistent questions by campaign groups, the IPT dropped a bombshell in February 2015. It ruled that until 5 December 2014, the GCHQ approach to intelligence obtained by the NSA, was unlawful. This was the first time that a British court has made a ruling against a broad activity by one of the UK Intelligence and Security Services. This constituted a major reversal for GCHQ, given the strong emphasis that it has placed on ’lawfulness’ since the 1990s. The availability of public knowledge about the programme and its formal avowal has now rendered it lawful. The ultimate question here is how much information about the practices of GCHQ needs to be made available in order to allow citizens a convincing system for redress - as required by the European Court. The IPT ruling has nicely captured the broader paradox of accountability for intelligence, insisting that a secret system of surveillance cannot be really secret - and so must be made known to the public in outline.

The campaign groups have been rather selective in their celebration of the IPT’s February 2015 findings. The IPT judgement does not mean that the government was engaged in the worst implications of Snowden’s disclosures, such as unlimited mass surveillance. In fact the IPT was at pains to say the opposite is the case: that surveillance powers are used only against those who seem to threaten the security of the UK. However, the definition of such a threat rests with officials.

9.4 The Role of Campaign Groups and Activists

Many of the campaign groups in the UK have tended to emphasise mass surveillance and “total” spying by NSA and GCHQ. Unsurprisingly, government has been inclined to resist this assertion, arguing instead that they only require “mass access”. The point about whether action by an algorithm or by a human being constitutes “surveillance” has proved to be a notably philosophical issue. It also underlines the problems of definition and technical understanding a realm that is changing fast.

Most of the larger campaign groups have deployed legal teams consisting of experienced human rights lawyers. These broadly agree that the primary defence of civil liberties in this area will be delivered by meaningful reform of RIPA, together with the energetic enforcement of its regulations and restrictions, not by the enhacement of parliamentary oversight committees. There is also a consensus that the distinction between contents and communications data requires better clarification. Communications data, which receives much less protection under RIPA than contents data, now encompasses websites visited, social media address lists and many other significant elements of a citizen’s online identity. Most insist that the UK needs a change in the law to afford much greater protection in this area. Globalization is also an issue and so the distinction between internal and external communications will also need to be considered.

There has been surprisingly little interest in European developments, including the “Safe Harbour” judgement eagerly awaited from the ECHR. Most UK groups are agreed that better safeguards regarding the usage of bulk data are required including transfer of data to third-party powers, but tend to see this as a national rather than a regional issue. At present this is largely at the discretion of ministers and there is pressure for RIPA to take more account of ECHR Article 8 and even Article 10 on Freedom of Expression here. More fundamentally, laws on espionage and officials secrets, which currently forbid suspects from explaining their purpose to a court, seem increasingly at odds with Article 10. Governments are likely to resist any change here, demanding transparency from their citizens but not for themselves. Either way, we are likely to see more large-scale leaking and more technologically enabled Edward Snowdens.

Liberty, one the of the UK's most prominent civil liberties organisations, has also focused on the reform of the surveillance framework provided by RIPA and have been especially worried that its provisions are circumvented by exchange with foreign agencies. They rightly observe that fact that this matter has only emerged through the Snowden revelations raises significant concern as to the effectiveness of oversight mechanisms and inquiry bodies, including IRTL and IPT. They further argue that the surveillance legislative framework must now be revisited to address the different types of information and to emphasise "retail" rather than "wholesale" surveillance. There needs to be a system that offers additional agreements for information sharing between security agencies that are transparent and that will prevent the agencies from circumventing safeguards in an ingenious way. Judicial authorisation for surveillance rather than ministerial warrants is also viewed as central by *Liberty* (Ogilvie & Sankey, 2014).

In short, the mainstream campaign groups on privacy and the IRTL share much common ground. But beyond the pressure groups there are the further shores of digital activism. Hitherto, these fringe groups were often ignored by the mainstream media and by academic debate. But we are likely to see digital activism entering a phase of mainstreaming as 'politics as usual' over the next decade. If the citizen watching the state, the so called "reverse gaze", has established itself as normal over the last ten years, then perhaps DIY cyber-war is the next frontier? Most likely the higher level character of conflict in digital networks will intensify to the extent that digital activism and cyber conflict will begin to merge. One of the interesting phenomenon we have observed is that, where states are today, proliferating technology allows the individual citizen and protester to go tomorrow (Karatzogianni 2015).

10.Conclusions and Recommendations

10.1 From creating security to "curating" security.

Government needs to look ten years ahead. We are moving into a new environment in which we need to think through the social implications of knowledge-intensive security. Much of the Snowden episode was driven by a realisation that intelligence is no longer owned by the intelligence agencies - instead it is owned by large corporations that are often multinational and it may even be owned by individual citizens. In the future, large data sets will also be owned and analysed by small groups even individuals. In the digital realm, states will no longer "create" security they will merely co-ordinate and "curate" security (Hall & Zarro 2012).

10.2 Preparing for a more Transparent society.

The advent of a world in which everything around us gathers data means that we must prepare for a world in which individuals have less privacy, corporations have less confidentiality and governments are increasingly bereft of secrecy. The challenge is to ensure that knowledge-intensive security promotes a more open, prosperous and sustainable society. Transparency has its own problems, but we are unlikely to be able to turn back the clock. Instead, we need to ensure that our data is owned horizontally, openly and democratically. We need to think hard about the growing role corporations will play and what the implications are for democratic control over security. An end to widespread spying is unlikely, instead we need much better oversight and regulation that will ensure stronger public confidence.

10.3 Authoritarian states and criminals.

Privacy groups have argued that that personal data should only be collected for national security purposes with the consent of those targeted or through the application of a court order granted on the basis of reasonable suspicion. Unfortunately, the Snowden revelations have triggered a spying arms race and many authoritarian and semi-authoritarian states that did not have systems like “Tempora” and “Prism” are now acquiring them. Perversely, Snowden’s revelations seem to have had the unintended effect of accelerating the global volume of spying on individuals. Efforts to prevent the export of surveillance technology to authoritarian regimes have proved less than ineffective. Analytical technology is now proliferating and spying is becoming cheaper and easier on an ever bigger scale. Citizens will increasingly turn to their own national security agencies to offer them some protection against the worst of this malignant activity from elsewhere, together with cybercrime.

10.4 Improved oversight and informal oversight

In the short term, the UK needs much better judicial control mechanisms in which warrants are approved by a court not a minister, and ideally its also needs an Inspector-General. This would offset the lacklustre performance of the ISC. The limited changes to ministerial warrants proposed by the ISC offer little by way of enhanced protection. The most controversial area will probably be around the decline of government secrecy. Government will resist providing credible, effective protection for whistle-blowers exposing unlawful surveillance activities. Certainly, “regulation by revelation” is an uncertain business which often has unintended consequences. The most effective measure the EU might take to enhance oversight would be introduce more legal protection in this area, but national governments will seek to apply caveats similar to those imposed in the USA to isolate national security issues from whistle-blower protection.

10.5 International Oversight

One of the most challenging areas is information sharing between intelligence agencies across national borders and intelligence operations that are carried out on a multinational basis. National inquiries find these especially challenging to investigate. An Inspector-General with a multinational remit would be the best solution to this taxing problem. Again, national governments will not like this, but they will have to confront the fact that if they do not provide effective multinational oversight, then human rights lawyers, media and international courts, often working together, will step into this vacant space and gleefully do it for them.

10.6 End to End Encryption

In the long term, we are likely to see energetic technical efforts by the scientific community to roll back surveillance. ISP providers, Internet businesses and computer hardware manufacturers have been vexed by the behaviour of NSA in particular. A new generation of cryptographers and researchers are now dedicated to promoting end-to-end encrypted communications. The 1990s Clipper Chip episode suggests that governments will prove powerless to stop this development in the long term. The UK Prime Minister, David Cameron, wishes all services using such encryption to provide governments, intelligence services and law enforcement with back doors that would give them the ability to intercept communications. In reality, what we are likely to see is more limited government access to call content and more expansive access to call data or geo-locational information. Historically, the parameters of intelligence gathering and surveillance have tended to be driven by technology, not by law or policy. One suspects that this where the new technology will take us over the next ten years. Perhaps a situation where meta-data is more widely available, but content is hard to access, will provide an uneasy truce in the accelerating wars over privacy and secrecy.

Appendix 1: Public Documents discussed (copies provided)

1.*'A Question of Trust': Report of The Investigatory Powers Review,* by David Anderson Q.C. Independent Reviewer of Terrorism Legislation, June 2015 (IRTL 2015)

https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

2.Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, HC 1075 (ISC 2015)

http://isc.independent.gov.uk/committee-reports/special-reports

3.Intelligence and Security Committee of Parliament, *Annual Report 2013–2014*, 25 November 2014, HC 794 (ISC 2014)

http://isc.independent.gov.uk/committee-reports/annual-reports

4.The Investigatory Powers Tribunal, *Information Leaflet for Human Rights Claim Form T1*

http://www.ipt-uk.com/docs/InformationLeafletT1_180614.pdf

5.Investigatory Powers Tribunal Report 2010

http://webarchive.nationalarchives.gov.uk/20140911100308/http://consultation.cabinetoffice.gov.uk/justiceandsecurity/wp-content/uploads/2012/05_Investigatory%20Powers%20Tribunal.pdf

6.Investigatory Powers Tribunal, [2015] UKIPTrib 13_77-HLiberty (The National Council of Civil Liberties) & Others Claimants and The Secretary of State for Foreign and Commonwealth Affairs & Others, 6 February 2015 (IPT 2015)

http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf

7.Privacy International/Amnesty International, *Two Years After Snowden: Final* Report. July 2015.

https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN.pdf

8.Don't Spy On Us, *Response to the inquiries into privacy and surveillance*, September 2015

https://www.dontspyonus.org.uk/assets/site/dontspyonus/files/DSOU_Response_report_WEB.pdf

9.Liberty's briefing on 'A Question of Trust: The Report of the Investigatory Powers Review' June 2015

https://www.liberty-human-rights.org.uk/policy

References

Agar, J. 2003. *Constant Touch: A Global History of the Mobile Phone*. London, Counterpoint.

Aid, M.M., 2012. *Intel Wars: The Secret History of the Fight Against Terror*. New York, Bloomsbury.

Alexander, M.S. 1998) 'Knowing Your Friends, Assessing Your Allies - Perspectives on Intra-Alliance Intelligence'. *Intelligence and National Security,* 13/1: 1-17.

Aldrich, R.J. 2005. 'Whitehall and the Iraq War: the UK's Four Intelligence Enquiries'. *Irish Studies in International Affairs*, 16: 73-88.

Aldrich, R.J. 2009. 'Regulation by Revelation? Intelligence, Transparency and the Media', in R. Dover & M. Goodman (eds.) *Spinning Intelligence: Why Intelligence Needs the Media, Why the Media Needs Intelligence.* New York, Columbia University Press, pp.13-37.

Aldrich, R.J. 2010. *GCHQ: The Untold Story of Britain's Most Secret Intelligence Agency*, London, HarperCollins.

Aldrich, R.J. & Cormac, R. 2016. *Behind the Black Door: The British Prime Minister and Secret Intelligence*, forthcoming London, HarperCollins, forthcoming August 2016.

Allen, N. and Peter Foster. 2005, 'Former senior CIA official says waterboarding was "torture"', *Telegraph,* 3 August 2015.

Anderson, D. 2014. 'The independent review of terrorism laws; Searchlight or Veil?', *Public Law*. 403-420.

Andrew, C. 2009. *Defence of the Realm: The Authorised History of the Security Service*, Allen Lane.

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

Andrew, C. & Mitrokin, V. 1999. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. NY, Basic Books.

Appelbaum, J. Stark, H. Rosenbach, M. & Schindler, J. 2013. 'Berlin Complains: Did US Tap Chancellor Merkel's Mobile Phone?' *Der Spiegel*, 23 October 2013.

Axford, Barrie. 2011. 'Talk About a Revolution: Social Media and the MENA Uprisings.' *Globalizations*, 8/5, 681-686.

Bamford, B.W.C. 2005. 'The United Kingdom's "War Against Terrorism"'. *Terrorism and Political Violence,* 16/4: 737-56.

Barnett, H. 2002. *Britain Unwrapped: Government and Constitution Explained*. London, Penguin.

Belasco, A., and Daggett, S. 2004. CRS Report RL32422, 'The Administration's FY2005 Request for $25 Billion for Operations in Iraq and Afghanistan: Precedents, Options, and Congressional Action', 22 July 2004.

Bochel, H., Andrew Defty & Jane Kirkpatrick. 2014. *Watching the Watchers: Parliament and the Intelligence Service*s, London, Palgave Macmillan.

Born, H. and I. Leigh (eds.) 2010, *International Intelligence Co-operation and Accountabilit*y, London, Routledge.

Bowcott. O. 2015.'UK-US surveillance regime was unlawful "for seven years"', *The Guardian,* 6 February 2015.

Brin, D. 1999. *The Transparent Society: Will Technology Force Us To Choose Between Privacy and Freedom?* New York, Basic Books.

Brooke, H. 2010. 'The data deluge is coming ...' Jonathan Powell, Alan Rusbridger, David Leigh, Timothy Garton-Ash and Heather Brooke discuss the leaked US embassy cables. 28 November 2010.

Lord Brown of Eaton-Under-Heywood. 2007. *Report of the Intelligence Services Commissioner for 2005-2006*, HC 314.

Butler, Lord. 2004. *Review of Intelligence on Weapons of Mass Destruction*, London, The Stationery Office.

Cabinet Office. 2002. *Intelligence Oversight*, London, The Stationery Office.

Campbell, D. & Ramesh, R. 2006. 'Pakistan says 'ringleader' admits link with al-Qaida'. *Guardian*, 14 August 2006.

Hall, Catherine & Zarro, Michael. 2012. 'Social curation on the website Pinterest.com'. *Proceedings of the American Society for Information Science and Technology*, 49/1: 1–9.

Chirinos, A. 2005. 'Finding the Balance Between Liberty and Security: The Lords' Decision on Britain's Anti-Terrorism Act'. *Harvard Human Rights Journal*, 18/2: 265-276.

Christou, G., 2015. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, London, Palgrave.

Collins, K., 2015. 'MPs: replace all laws governing UK intelligence agencies', *Wired*, 12 March 2015

Danchev, A. 2006. 'Accomplicity: Britain, Torture and Terror': *The British Journal of Politics and International Relations*, 8/4: 587–601.

Dandeker, C. 1990. *Surveillance, power, and modernity*. NY, St. Martin's.

Davies, P. H. J. 2004. 'Intelligence Culture and Intelligence Failure in Britain and the United States'. *Cambridge Review of International Affairs*, 17/3: 495-520.

Davies, P. H. J. 2013. *Intelligence and Government in Britain and the United States: A Comparative Perspective*. NY, Praeger.

Defty, A. 2008. 'Educating Parliamentarians about Intelligence: The role of the British Intelligence and Security Committee', *Parliamentary Affairs*, 61/4: 621-41.

Fenwick, H. 2002. *The Anti-Terrorism, Crime and Security Act 2001: A Proportionate Response to 11 September?* Modern Law Review, 65: 724-762.

Foreign Affairs Committee. 2004. *Implications for the Work of the House and its Committees of the Government's Lack of Co-operation with the Foreign Affairs Committee's Inquiry into The Decision to go to War in Iraq*, London, The Stationery Office.

Gearty, C. 1991. *Terror*, London, Faber & Faber.

Gerges, F. 2005. *The Far Enemy: Why Jihad Went Global*. Cambridge. Cambridge University Press.

Gill, P. 1996. 'Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community'. *Intelligence and National Security*, 11/2: 313-331.

Gill, P. and Phythian, M. 2006. *Intelligence in an Insecure World*, Cambridge, Polity Press.

Glees, A. and Davies, P. H. 2006. 'Intelligence, Iraq and the limits of legislative accountability during political crisis'. *Intelligence and National Security* 21/5: 848-883.

Glees, A., Davies, P. and Morrison, J. 2006. *The Open Side of Secrecy: Britain's Intelligence and Security Committee*. London, The Social Affairs Unit.

Gregory, F. & Wilkinson, P. 2005. Riding Pillion for Tackling Terrorism is a High-Risk Policy, ISP/NSC Briefing Paper 05/01, Chatham House http://www.riia - org/pdf/research/niisBPsecurity.pdf

Hakimi, M. 2007. 'The Council of Europe Addresses CIA Rendition and Detention Program,' *American Journal of International Law,* 101/2: 442-52.

Hammond, A. & R.J. Aldrich. 2014. 'Securing Freedom: Obama, the NSA and American Foreign Policy', in Inderjeet Parmar, Linda B. Miller, Mark Ledwidge (eds.) *Obama and the World: New Directions in US Foreign Policy,* London, Routledge, pp.303-14.

Harding, L. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man*, Guardian Faber.

Harfield, C. 2006. 'SOCA: A Paradigm Shift in British Policing'. *British Journal of Criminology*. 46: 743-61.

Harris, M. et al. 2014. *Megacities and The United States Army: Preparing For A Complex And Uncertain Future*, Chief of Staff of the Army Strategic Studies Group.

Harris, P. 2012. 'Drone wars and state secrecy – how Barack Obama became a hardliner', *Guardian,* 2 June 2012.

Held, D. 1995. *Democracy and the Global Order: From the Modern State to Cosmopolitan Governance,* Stanford, Stanford University Press.

Herrington, L., 2015. 'British Islamic extremist terrorism: the declining significance of Al-Qaeda and Pakistan', International Affairs, 91/1: 17–35.

Herrington, L. & Aldrich R. 2013. 'The Future of Cyber-Resilience in an Age of Global Complexity', *Politics*, 33/4, 299–310.

Home Affairs Committee. 1999. *Accountability of the Security Service*, London, The Stationery Office.

Hosein, I. and Eriksson, J. 2010. 'International policy dynamics and the regulation of data flows: bypassing domestic restrictions, in Eriksson, J. and Giacomello, G., (eds.) *International Relations and Security in the Digital Age,* London and New York, Routledge. Pp.158-72.

Intelligence and Security Committee. 2003. *Iraqi Weapons of Mass Destruction: Intelligence and Assessmen*ts, London, The Stationery Office.

Intelligence and Security Committee. 2009a. *Could 7/7 have been prevented? Review of the intelligence on the London terrorist attacks on 7 July 2005*, London: The Stationery Office.

Jeffery, K. 2011. *MI6: The History of the Secret Intelligence Service 1909-1949*, London, Bloomsbury.

Johnson, L.K. 1986. 'The CIA and the media', *Intelligence and National Security*, 1/2: 143–69.

Joint Committee on Human Rights. 2006. *Counter-Terrorism Policy and Human Rights: Prosecution and Pre-Charge Detention*, London, The Stationery Office.

Joint Committee on Human Rights. 2009. *Allegations of UK complicity in torture*, London, The Stationery Office.

Kalathil, S. and Taylor C. Boas. 2003. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*, New York, Carnegie Endowment.

Kaldor, M. 2013. *New and Old Wars: Organised Violence in a Global Era,* Cambridge, Polity.

Karatzogianni, A. 2015. *Firebrand Waves of Digital Activism 1994-2014 The Rise and Spread of Hacktivism and Cyberconflict,* London and New York, Palgrave.

Karatzogianni, A., (ed.) 2009. *Cyber Conflict and Global Politics,* London and New York, Routledge.

Lander, S. 2004. 'International Intelligence Co-operation: An Inside Perspective', *Cambridge Review of International Affairs.* 17/3 (2004): 481-93.

Lefebvre, S. 2003. 'The Difficulties and Dilemma of International Intelligence Cooperation', *International Journal of Intelligence and Counterintelligence,* 16/4: 527-42.

Leigh, I. & Lustgarten, L. 1991. 'Employment, Justice and Detente: The Reform of Vetting'. *The Modern Law Review*, 54: 613-642.

Leigh, I. 2005. 'The UK's Intelligence and Security Committee', in Born, H. And Caparini, M. (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Aldershot, Ashgate, pp.177-94.

Leigh, I. 2005. 'Accountability of Security and Intelligence in the United Kingdom'. in H. Born. L. K. Johnson & I. Leigh *Who's Watching the Spies: Establish Intelligence Service Accountability*. ed.. Washington DC, Potomac, pp. 79-98

Leppard, D. 2009. 'Internet firms resist ministers' plan to spy on every e-mail', *Sunday Times*, 3 August 2009.

Libicki, M.C. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. NewYork, Cambridge University Press.

Lindsey, R.A. 2013. 'What the Arab Spring Tells Us About the Future of Social Media in Revolutionary Movements', *Small War Journal.*

London Assembly. 2005. 7 July Review Committee, Transcript of Item 3: 7 July – Lessons Learned, comments of Malcolm Baker, Superintendent, Anti-Terrorist Branch, Metropolitan Police Service, 1 December 2005.

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

Manningham-Buller, E. 2007. 'The International Terrorist Threat to the United Kingdom', in Peter Hennessy (ed.) *The New Protective State*. London, Continuum, pp.66-73.

Mathieson, S. 2005. UK seeks all-EU traffic data retention. *Computer Fraud and Security*, 7: 1-2.

McCrisken, Trevor. 2011. 'Ten years on: Obama's war on terrorism in rhetoric and practice', *International Affairs*, 87/4: 781–801.

Moore, Martin. 2014. 'RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework. *The Political Quarterly,* 85/2 (2014): 125-132**.**

Moran, C. 2013. *Classified: Secrecy and the State in Modern Britain*, Cambridge, Cambridge University Press.

Moran, J. 2006. State Power in the war on Terror: A comparative analysis of the UK and USA. *Crime, Law and Social Change*, 44/2: 335-59.

Moore, M. 2014. 'RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework', The Political Quarterly 85/2: 125–132.

Morrison, J.N.L. 2008. 'Political Supervision of Intelligence Services in the United Kingdom. Steve Tsang (ed.), *Intelligence and Human Rights in the Era of Global Terrorism*. Stanford: Stanford University Press, pp.158-170.

Mullin, C. 2009. *A View From The Foothills: The Diaries of Chris Mullin*, London, Profile.

Nagyfejeo, E., 2014. 'Transatlantic collaboration in countering cyber terrorism', in Lee Jarvis & S. McDonald (eds.) *Terrorism Online: Politics, Law and Technology*. London, Routlegde, pp, 144-73.

Naim, M. 2005. *Illicit: How Smugglers, Traffickers and Copycats are Highjacking the Global Economy* London, William Heinemann.

National Criminal Intelligence Service. 2000. *The National Intelligence Model*. London, National Criminal Intelligence Service.

Ogilvie, S. & Isabella Sankey. 2014. *Liberty's submission to the Reviewer of Terrorism's Investigatory Powers Review*, November 2014.

Omand , D., 2010. *Securing the State*, London, Hurst.

Omand, D. and Miller, Carl. 2012. '#Intelligence', London, Demos.

Omand, D. 2004. Emergency Planning, Security and Business Continuity. *RUSI Jo*urnal, 149/4: 26-33.

Omand, D. 2005. 'Countering International terrorism: The use of strategy'. *Survival,* 47/1: 107-116.

Patten, C. 2005. *Not Quite the Diplomat: Home Truths About World Affairs*, London, Allen Lane.

Phythian, M. 2007. 'The British Experience with Intelligence Accountability', *Intelligence and National Security*, 22/1: 75-99.

PRGICT, 2013. *Liberty and Security in A Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12 December. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

Priest, D., 2005. 'CIA Holds Terror Suspects in Secret Prisons', *Washington Post*, November 22, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html

Priest, D. and Arkin, W. 2012. *Top Secret America: The Rise of the New American Security State,* New York, Little, Brown and Co.

Pythian, M. 2005. Intelligence, Policy-Making and the 7 July London bombings. *Crime, Law and Social Change.* 44: 361-85.

RCUK. 2015, 'RCUK Policy and Guidelines on Governance of Good Research Conduct', July 2015 http://www.rcuk.ac.uk/about/aboutrcuk/aims/units/aasg/about/ethics/

Rees, W. 2006. *Transatlantic Security Cooperation: Drugs, Crime and. Terrorism in the Twenty-First Cent*ury. London, Routledge.

Rees, W. and Aldrich, R.J. 2005. Contending cultures of counter-terrorism: divergence or convergence? *International Affairs*, 81/4: 905-24.

Reveron, D.S. 2006. 'Old Allies, New Friends: Intelligence-Sharing in the War on Terror', *Orbis* 50/3: 453-468.

Rice, G. & Thomas, T. 1997. 'Men in black: With MI5 now moving in on the drug trade'. *Druglink*, 12: 14-15.

Rovner, J. 2013. 'Intelligence in the Twitter Age', *International Journal of Intelligence and CounterIntelligence*, 26/2: 260-71.

Rudner, M. 2004. 'Hunters and Gatherers: The Intelligence Coalition against Islamic Terrorism', *International Journal of Intelligence and Counterintelligence* 17/2: 193-230.

Runciman, W.G. (ed.) 2004. *Hutton and Butler: Lifting the Lid on the Workings of Power* London, British Academy/Oxford University Press.

Scholte, J.A. 2000. *Globalization: A Critical Introduction,* New York, St. Martin's.

Shane, S. 2012. 'Cost to Protect U.S. Secrets Doubles to Over $11 Billion', *New York Times*, 2 July 2012.

Shane, Scott. 2012. 'Shifting Mood May End Blank Check for US Security Efforts.' *New York Times*, 24 October 2012.

Shiraz, Z. (2013) 'Drugs and Dirty Wars: Intelligence Cooperation in the Global South,' *Third World Quarterly*, 34/10: 1749-1766.

Sims, J.E. 2006. 'Foreign Intelligence Liaison: Devils, Deals, and Details', *International Journal of Intelligence and CounterIntelligence*, 19/1: 195-217.

Smith, R. 2007. *The Utility of Force: The Art of War in the Modern World*, NY, Knopf.

Sommer, P. and Hosein, G. 2009. *Briefing on the Internet Modernisation Programme*, PEN paper 5, LSE.

Spiegel Staff. 2013 'Embassy Espionage: The NSA's Secret Spy Hub in Berlin', *Der Spiegel*, 27 October 2013.

Verkaik, R. and Morris, N. 2008. 'Exclusive: storm over Big Brother Database'*, Independent*, 5 October 2008

Wada, K. 2002. Outline of Anti-Terrorism Legislation in Foreign Countries. *Journal of Police Science*, 55/1: 51-96.

Walker, C. 2005. Intelligence and anti-terrorism legislation in the United Kingdom. *Crime, Law and Social Change*, 44: 387-422.

Walker, C. 2014. submissions to Independent National Security Legislation Monitor Repeal Bill 2014 [Provisions] Submission 9.

Acknowledgements

I wish to acknowledge support from AHRC Research Grant, 'Landscapes of Secrecy: The Central Intelligence Agency and the contested record of US foreign policy, 1947-2001', (2008-11) (AH/F018444/1) and also AHRC Follow-on Funding Grant, ‘Enhancing Openness and Explaining Secrecy: Policy Lessons from the Declassification and Management of US Intelligence and Security Records’, (2011-12) (AH/J001856/1). I would also like to thank friends and colleagues in the Department of Politics and International Studies (PaIS) and the Cyber Security GRP at the University of Warwick, together with many other individuals, for discussing these matters with me. Opinions, errors and omissions are my responsibility alone.

06.10.15