**Researching the Deep State: Surveillance, Politics, and Dissent**

The purpose of this Chapter is to develop a working methodology for the use of those academics, investigative journalists, and political activists who wish to conduct credible research into that nexus of forces known as the ‘deep state’. While it is possible to identify a number of viable techniques for use in this field, it is also important to consider both the risks, and the inherent limitations of conducting this type of research.

First, in terms of risk, the analyst has be sensitive to the particular types of information that he or she might disclose, since the potential consequences of disseminating state secrets within the public domain (deliberately or otherwise) can be considerable. This risk has to be balanced against the possible benefits to the ‘public interest’, but the precise repercussions of conducting (and then publishing) research into the practices of the intelligence community might not be apparent for many years. The limitations, meanwhile, of investigating the deep state might include the existence of powerful barriers such as official secrecy, which forces the researcher to pursue creative responses to bureaucratic red-tape. Another major ordeal is having to work with rescinded or redacted data sets, which means having to identify useful material where state censorship has left only minor hints in the text.

These issues do not exhaust the practical challenges posed by this type of research, which extend to the basic ability to interact productively and respectfully with one’s sources. In essence, the risks that might be faced are usually proportionate to the scope of the research being done. This Chapter, therefore, elaborates on some of the popular approaches used in this field, in addition to describing what is perceived to be good journalistic and academic practice, based upon the insights of those working in this area. Within the course of this exploration, I examine the methods of deep state research undertaken by academics such as Monahan (2009), Newkirk (2010), and Monaghan and Walby (2012). It also), while also considering the techniques used by journalists such as Campbell (1976), Greenwald (2013), and Evans (2009), and the risks faced by whistle-blowers such as Edward Snowden and Julian Assange.

**The Contemporary Deep State**

In terms of popular culture, the notion of the deep state has often been typified as a separate entity existing alongside the visible, conventional state; as a shadow government that operates behind the facade of everyday politics; or as a clandestine group of political and commercial interests that seek to manipulate public opinion, trade and commerce. Most recently it has been identified as an international consortium of agencies whose ubiquitous use of surveillance now forms *i)* one of the largest growth enterprises in the world (as an ‘intelligence-industrial’ complex), and *ii)*, controls the flow of digital information and thus the machinations of contemporary power (Wilson, 2009).

In an International context, news headlines regarding the activities of the deep state have in recent years been dominated by coverage of the secret intelligence programmes, exposed by Edward Snowden in 2013. On 7 July 2013 the *Guardian* newspaper revealed that the United States of America had been conducting mass surveillance of the American population, which included the interception of internet streams and the monitoring of private telephone calls (Greenwald, 2013). The National Security Agency (NSA) was largely responsible for what many citizens have since considered to be a flagrant disregard for personal privacy, and a gross misuse of state powers, in which emails, conventional and online/video calls, instant messaging services, and internet searches were all accessed by NSA operatives without any legal warrant (Shubber, 2013). The clandestine intelligence programme known as PRISM was revealed when Snowden (a former NSA contractor) leaked confidential documents to International press agencies, thus blowing the whistle on the unrestrained (and unregulated) use of mass surveillance. The implications of Snowden’s revelations were indeed wide-ranging. In addition to the unrestrained surveillance of the American population, Snowden’s documents also disclosed that a number of other agencies had been operating under the same *modus operandi* in other Western powers.

In the UK, an equivalent programme known as TEMPORA was revealed by Snowden via the *Guardian* newspaper (MacAskill, *et al*, 2013). The British signals intelligence agency, Government Communications Headquarters (GCHQ) had plugged itself into the fibre optic cables that carry internet communications between the USA and continental Europe, under a secret agreement made with the NSA (Shubber, 2013). The purpose of this covert programme was to gather signals intelligence from every connected part of the world. This included the surveillance of military, political, commercial, and domestic targets on a massive scale, since practically the whole of the world’s internet usage passes through America. Yet, spying on the world’s population is in itself nothing new.

Investigative journalist Duncan Campbell first drew public attention to the activities of GCHQ in 1976 and, during 1988, exposed a programme codenamed ECHELON in which British, Commonwealth, and American security allies had been intercepting telecommunications signals for nearly thirty years (Campbell, 1976, 1988). The ECHELON programme was a joint venture between British, Australian, Canadian, New Zealand, and American security services, who were working under an initiative known as FIVE EYES (a reference to the initial five stakeholders). The point here is that contemporary surveillance projects such as TEMPORA and PRISM represent part of a hidden history of the deep state which the general population is rarely privileged to observe. At first glance the intelligence programmes discussed in this Chapter appear less grandiose in scale than those exposed by Snowden or Campbell, but they do, however, form part of a wider surveillance strategy in the West that attempts to detect and monitor all forms of terrorism (or terrorist-type activity). Many such programmes are now commonplace throughout Europe as well as appearing in the USA and the Commonwealth. They are enacted principally through organisations such as the Department for Homeland Security in America, by Europol, and by British intelligence (Jones, 2014).

**Surveillance, Politics, and Dissent**

In 2009 Monahan and Palmer published the first of a series of scholarly articles on the emerging surveillance networks of the United States of America (2009: 617-636). These sites were later defined as forming a ‘fusion intelligence complex’, in which the Department for Homeland Security (DHS) had commissioned a series of new facilities to monitor threats posed by terrorist organisations and from far-left, or right-wing political groups (Newkirk, 2010). In what became known as DHS Fusion Intelligence Centres, public and private sector interests were represented by a number of hybrid surveillance hubs that were composed of both federal and corporate employees. In addition to their conventional role (i.e., to detect and prevent serious crimes such as international or domestic terrorism), the fusion centres were also concerned with protecting sites of critical national importance - including telecommunications and utilities providers. It was believed that such facilities represented key terrorist targets, and unless they were protected, would render vital public services useless during a federal emergency. However, the problem for a number of social movements was that the operation of power stations, the expansion of public transportation and aviation networks, and global economics, are contentious issues that have been the cause of numerous public disputes.

As a result of this joint security venture, the fusion centre initiative crept into the domain of ‘public order’ affairs, in addition to countering the threat posed by terrorism. To problematise the issue of fusion-led intelligence, a number of scholars have observed that the commercial and public concerns monitored by such facilities, have led to a conflict of interests between state and corporate surveillance, and Western ‘civil liberties’. In other words, the encroachment of fusion centre surveillance into the public order domain has led to the conflation of political activism and terrorism as the target for these new hybrid intelligence agencies. According to Monahan:

Fusion centre threat assessments lend themselves to profiling along lines of race, religion, and political affiliation. Their products are not impartial assessments of terrorist threats, but rather betray biases against individuals or groups who deviate from—or challenge—the status quo. (2010: 90)

Further issues are typified by the limited executive oversight (where it exists at all) of fusion centre surveillance, and the routine dissemination of sensitive personal data to third party organisations (Monahan and Palmer, 2009: 631). An equivalent concern has been the profound lack of transparency and public awareness of the operational procedures of these joint security ventures, for ‘the details of these relationships are shrouded in secrecy’ (*Ibid*: 619). Moreover, the way in which the designated targets of these institutions have been depicted, poses an even greater question for privacy advocates and campaigners alike. To put this into context, by 2015 there were over seventy-eight DHS fusion centres operating in the US alone, with significant interest being shown in the model by America’s overseas allies (DHS, 2016, and Jones, 2014). With regards to the mission creep of fusion centre surveillance and the comparative profiling of both terrorists and activists under an equivalent threat matrix, the spread of these institutions equates to the criminalisation of social movements in the west.

In terms of the legitimacy of fusion centre surveillance, the role of these institutions within civil contingencies and risk aversion doctrine has aligned cause-led activism and legitimate public protest, with domestic and international forms of terrorism. By way of theorising this affiliation, Walby and Monaghan have used the term ‘multi-issue extremism’ (MIE) which is widely used by Canada’s equivalent to the DHS (the Canadian Security Intelligence Service) and by its comparative fusion centre complex (2012: 113). The use of multi-issue extremism serves as an all-purpose term, through which law enforcement agencies are able to conduct counter-terrorism style operations against ordinary campaign groups. In terms of fusion centre surveillance, this has led to the interception of domestic communications, and to other forms of clandestine oversight. Consequently, the said intelligence also provides a justification for law enforcement agencies to run covert infiltration operations within such groups, which provides officials with an additional insight into the activities of social movements (Monahan, 2010: 89).

Although the paradigm outlined above differs from one territory to the next, there is an equivalent ‘multi-issue extremism’ (MIE) discourse being touted by fusion centres throughout the west (Harbisher, 2015). In Canada this has been investigated by Walby and Monaghan in relation to the nation’s Integrated Security Units (ISUs) and the Integrated Threat Assessment Centre (ITAC). In one example, cited by Walby and Monaghan, opposition to the Vancouver 2010 Olympic and Paralympic Games (offered by the Olympic resistance movement) resulted in a number of agencies attempting to police the threat as an MIE:

On the ground, the diverse Olympic resistance movement began mobilising popular opposition to the Games. This opposition began to result in intelligence material gathered from various local policing agencies. ITAC began to re-code the diverse branches of the emerging movement against the Olympic Games in the discursive framework of ‘extremism’ and then ‘terrorism’. (2012: 148)

In the Unites States, Monahan’s research into the fusion centre complex has revealed similar findings. In the second instance of MIE discourse, both race-orientated and student protest groups were depicted, in 2009, as posing an extremist threat to the state of Virginia. In citing the risk as an MIE, Virginia’s threat assessment centre reported that many of these organisations were ‘recognized as a radicalization node for almost every type of extremist group’ (Monahan, 2010: 48). Between 2008 and 2009, the official response to this particular type of threat was furthermore outlined by the treatment of the American Civil Liberties Union (ALCU) by the Maryland Coordination and Analysis [fusion] Centre (MCAC). During an ALCU lawsuit over a freedom of information request, ‘the Maryland State Police had conducted covert investigations of at least 53 peace activists and anti-death penalty activists for a period of 14 months’, despite admissions by covert operatives of there being ‘no indication of violent activities or violent intentions on the part of group members’ (*Ibid*: 89).

In the UK, significant research has been conducted into this issue by investigative journalists Rob Evans, Paul Lewis, and Matthew Taylor from the *Guardian* newspaper (2009, and 2013). The British equivalent of an MIE is the term ‘domestic extremism’, which has been widely used by HM Constabulary as a means of shaping the public’s perception of social movements, and of controlling demonstrations. As with the UK’s overseas allies, the deployment of MIE classifications by intelligence agencies and law enforcement officials has been used to define campaign groups within civil contingencies doctrine as posing a threat equivalent to organisations such as al Qaeda. Although the UK is alleged to have only one official fusion intelligence centre, the Joint Threat Assessment Centre (which is a subdivision of GCHQ), local government authorities operate regional risk assessment centres, which also comply with Monahan and Palmer’s earlier paradigm. In this respect, the UK’s Local Resilience Forums (LRFs) coordinate different intelligence streams between regional contingency stakeholders. These include the police and emergency services, representatives from the private sector (often including their own in-house intelligence experts and security employees), and Local Government Authorities. Good evidence exists to suggest that the LRFs are equally accountable for disseminating MIE discourse into the public domain - as has been the case elsewhere in the West.

In 2006 for example, Local Government Authorities and emergency services attended a mass environmental protest at the Drax Power Station in Selby (North Yorkshire), which is one of the UK’s largest coal-powered electricity providers. Activists from the Camp for Climate Action group descended on the site which, on 31 August 2006, was attended by over 3000 police officers (Brown, 2006). During an otherwise peaceful demonstration, thirty-nine people, intent on closing the facility and disrupting its activities, were arrested for trying to break into the power station. North Yorkshire Police later claimed it was the ‘first time that domestic extremism had ever taken place in the county’, thus issuing an MIE categorisation for the event (North Yorkshire Local Resilience Forum, (2006). However, the bigger picture of political policing in the UK reveals not only that the notion of domestic extremism is a ‘common currency’ within the force, but that a number of dedicated police units had been commissioned to attend to such matters (Evans, Lewis, and Taylor, 2009: 6).

Under the operational aegis of the (now-defunct) Association of Chief Police Officers’ ‘Terrorism and Allied Matters group (ACPO-TAM)’,[[1]](#endnote-1) further divisions were created to police public protests including the National Public Order Intelligence Unit (NPOIU), the National Extremism Tactical Coordination Unit (NETCU), and the National Domestic Extremism Unit (NDEU). Many of these departments later merged into a new task force entitled the National Domestic Extremism and Disorder Intelligence Unit (NDEDIU) following a public scandal over the failed convictions of environmental activists in Nottingham (Jones, 2011). As a result of flawed intelligence provided by an undercover operative embedded in the environmental movement, a public enquiry into the use of Covert Human Intelligence Sources was called for. After two consecutive inquiries into the affair, the Rose report (2011: 5), and an investigation by the Independent Police Complaints Commission (IPCC, 2011: 5), it was revealed that two Operations (codenamed Pegasus and Aeroscope) had employed NPOIU officers to infiltrate environmental groups in the region. Operation Pegasus (circa, 2008) involved a number of agents who had been ordered to infiltrate groups of domestic extremists throughout the UK (*Ibid*). Operation Aeroscope was a localised investigation into campaign groups operating within the Nottinghamshire region, which resulted in over 100 campaigners being arrested at the Iona Independent School in Nottingham, based upon intelligence that campaigners were planning to assault a nearby power station in 2009 (*Ibid)*. The resulting public scandal, the press coverage, and the inquiries all ‘related to the infiltration of various domestic extremist groups’ by undercover police (*Ibid*). The nefarious practice of maintaining a covert identity was also brought into question following allegations by journalists, to the effect that, as part of their ruse, undercover agents had maintained personal relationships with campaigners for a number of years.

Further use of MIE discourse in the UK can be found in the depiction of the Occupy movement by City of London Police in 2011. In a letter distributed to companies within London’s business district, numerous organisations were warned of the on-going threat posed by terrorists and extremists. However, the memorandum made limited differentiation between the two categories of individual, and financial workers were asked to remain vigilant of the ‘suspected reconnaissance’ of empty buildings by anti-capitalist demonstrators (City of London Police, 2011). The letter depicted further risks to the business community such as a planned electrician’s strike by Balfour Beatty employees, and advised of potential direct action campaigns by the Stop Huntingdon Animal Cruelty animal rights group (SHAC). The letter framed these organisations as posing an equivalent threat to businesses as the Revolutionary Forces of Colombia, and al Qaeda, and even detailed a forthcoming demonstration by the Climate Justice Collective as posing a severe risk to trade and commerce (*Ibid*).

**Key Research Methods into the Deep State**

So far, this Chapter has outlined what a notional ‘deep state’ might consist of, in terms of its appearance in a number of intelligence agencies and secretive organisations, as well as the way in which they have framed public dissent as a manifestation of ‘multi-issue extremism’ (MIE). In order to gain a sense of how MIE discourse and fusion centre surveillance try to shape the world, or rather, how they present one account of the world according to the political objectives of the deep state. both MIE discourse and the institutions that disseminate it needs to be identified and examined. The purpose of this part of the Chapter is to consider how a number of investigative journalists and academics have arrived at these conclusions, and to determine which techniques were used in their research.

The background research for Monahan and Palmer’s ‘The Emerging Politics of DHS Fusion Centers’ (2009: 617-36), was pieced together using material gathered from a range of sources – as these articles often tend to be. In reality not only does a wider search for empirical evidence often yield surprising results, but it can also be thought of as good academic and journalistic practice. The belief that one should always attempt to verify the sources that have been used, and cross-reference them wherever possible, is generally sound advice. For their 2009 publication, Monahan and Palmer examined a number of different newspaper articles that were written between 2002 and 2008. They used the LexisNexis search engine to identify specific key words from newspapers and other such publications that existed during this period. Using this approach they were able to perform a qualitative analysis of news reports containing references to fusion centre surveillance in the USA. The criteria of the dates for examination were based on the year that the DHS was first commissioned, following which the DHS fusions centres started to emerge.

We conducted a LexisNexis search for articles mentioning both ‘homeland’ and ‘fusion center’, or those mentioning both ‘terrorism’ and ‘fusion center’, published between November 2002 and December 2008. November 2002 was chosen as a start date because the Department of Homeland Security was created then. The search returned 90 newspaper and magazine articles, 56 of which were deemed relevant, 49 of which were unique. (*Ibid*: 620)

Following the initial hits returned by their LexisNexis research (and the articles to which they corresponded), a wider Google search was undertaken as a means to discover key government documents from the same period. In terms of making a comparative analysis of the evidence that their initial research revealed, this was a good technique to employ - working on the premise that open governments make some of their activities public knowledge. This kind of data generally relates to the organisation of a nation’s security infrastructure and to the institutions involved, if nothing else.

During this type of investigation one of the main issues faced by both academics and reporters is the impenetrable language used by intelligence agencies and security providers. But of course this is one of the ways in which secret agendas or clandestine organisations remain hidden from public scrutiny and demands for executive oversight. However, as clandestine programmes are usually referred to by their codenames within official publications (as are the key agencies, actors, or initiatives involved), a simple lesson to be learned from this investigative strategy is that one can identify the organisations based on the specific aliases that are in use. For instance, following Monahan and Palmer’s preliminary research into the DHS, the fusion centre programme was also exposed. Yet, to problematize the investigation of the fusion centre complex throughout the west, a big part of the problem facing scholars and journalists alike, is that all these organisations (while they hold relatively true to Monahan and Palmer’s initial paradigm) have different operational names and inter-agency relationships. In this respect, the research strategy of triangulating one’s findings is an essential technique for gathering future data.

In Monaghan and Walby’s later investigation into Canada’s fusion intelligence complex (and the use of MIE discourse to demonise opposition to the 2010 Vancouver Games), an altogether different approach was used. The article employed Monahan and Palmer’s earlier qualitative methods, but in addition to examining news reports, it also used freedom of information requests to gather empirical data from official sources. In their examination of how Canada's Integrated Threat Assessment Centre deployed MIE classifications to defame social movements, Monaghan and Walby explained how ‘Access to Information Act (ATIA) requests’ were used to reveal how ‘policing and surveillance projects developed in preparation for three mega-events that recently took place in Canada’ (2012: 133).

From their findings it was determined that Canada’s fusion intelligence complex operates in much the same way as its continental and international allies. It consists of a number of regional surveillance hubs that coordinate streams of intelligence between different municipal, state, corporate, and law enforcement agencies. These include the Canadian Security and Intelligence Service (CSIS), the Integrated Threat Assessment Centre (ITAC), Integrated Security Units and Joint Intelligence Groups (ISU-JIG), and the Royal Canadian Mounted Police (RCMP). In 2003, the RCMP established the ISUs as a cross border, multi-agency task force designed to provide intelligence for mega events such as the Olympic Games and the G8/G20 political and economic summits. The ISUs were initially designed to collaborate with international partners such as the United States, by aligning military and domestic intelligence resources. The RCMP later amalgamated the ISUs with Canada’s Joint Intelligence Group, combining municipal and provincial police authorities, the CSIS, and the armed forces, under one operational framework. According to Monaghan and Walby, the ISU-JIG collaboration was later reincarnated as the ITAC, which continued much the same role in relation to the policing of mega events:

JIG issued its first ‘preliminary’ Threat Assessment related to the 2010 mega-events on 12 May 2005. Later, in a report from 1 April 2007, the JIG’s function is described as follows: ‘The JIG plans to develop a comprehensive public order portfolio to monitor and access high risk groups, individuals, and potential threats to Olympic-related events’. From its inception in 2005 until the 2010 mega-events, the JIG played a central role in coordinating security intelligence practices. Notably, however, after meetings in late 2006, it was decided that the editorial control of ‘Threat Assessments’ would be undertaken by a CSIS agency, known as the Integrated Threat Assessment Centre. (*Ibid*: 136)

From their investigation into fused corporate, military, and domestic policing resources, Monaghan and Walby were able to determine how these institutions (the ITAC in particular), used MIE categorisations to manage public order threats to mega events. Although the above institutions still played their unique individual roles – from coordinating intelligence resources to conducting actual covert operations, the ITAC’s editorial control of risk categorisations presented a consistent discourse to security and business partners, and of course to the Canadian public.

In addition to the research gleaned from official reports into the activities of groups such as ITAC, the aforementioned strategy of analysing media coverage of public order operations was used to determine ‘how intelligence agencies have blurred the categories of terrorism, extremism and activism into an aggregate threat matrix’ (*Ibid*: 133). To further their concerns regarding the reclassification of legitimate social movements and grass roots organisations as ‘extremist’, it was concluded that the CSIS had deliberately blurred ‘the protection of private property especially the property of Olympic corporate sponsors within the rubric of national security’ as a means to justify the surveillance of protest groups (*Ibid*: 144). According to Monaghan and Walby’s research, the mainstream media[[2]](#endnote-2) reported that ISU officers had used tactics such infiltration against campaign organisations, that they had visited specific activists at their private homes to serve as a warning not to interfere with the Olympic games, and had even ‘posed as bus drivers, inviting activists into their bus apparently headed to Olympic Torch Relay disruptions’ (*Ibid*: 149). The latter of these propositions frames covert ISU operations as COINTELPROs, as Counter-Intelligence Programmes designed to misdirect, misinform or simply interrupt any planned campaign actions. It was therefore observed that:

ISU officers [had] made numerous house-calls to prominent activists and critics before the Olympics. Between 3 and 5 June 2009, approximately 15 anti-Olympics activists were visited by approximately eight ISU members. The ISU also had covert officers that spent several years undercover with groups in British Columbia and Ontario. (*Ibid*: 137)

Notwithstanding, one of the main issues faced by those wishing to undertake deep state research are the limits placed on access to freedom of information requests, which are often denied on the grounds of National Security by intelligence agencies. Monaghan and Walby readily admit that their own ATIA requests were limited by various renditions of official secrecy, even to the extent that the ISU (*et al*) had lobbied the Canadian Government to place restrictions on public access to documents regarding its operations. The belief was that wider knowledge surrounding its operational practices would have *I)* severely hampered its capacity to police the Olympic games, and *ii)* that ‘such information [could] be put to nefarious counter-intelligence use by terrorist or protest groups’ (Walby and Monaghan, *Ibid*: 139).

In terms of investigating the UK’s fusion intelligence complex, research published by journalists such as Rob Evans, Paul Lewis and Matthew Taylor, and work conducted by scholars in this field, has framed much of the debate surrounding the fusion centre/MIE affair. Research strategies have included requests made under the *Freedom of Information Act 2000* to civil contingency and police partnerships, the use of official publications, the analysis of media publications, attendance at international conferences on policing and surveillance, and networking with authors and activists in this field. Of course, leaked intelligence reports and the use of additional materials disclosed by whistle-blowers such as Edward Snowden, also provides invaluable background into deep state organisations such as the NSA and GCHQ.

The British version of a fusion intelligence complex has been presented so far in terms of the public and private sector networks that were commissioned post-9/11 to protect the UK’s Critical National Infrastructure. But of course any investigation into the deep state must venture further than this. Under laws such as the *Civil Contingencies Act 2004* and the UK’s counter terrorism strategy (known as CONTEST), a gradual blurring of lines ‘between terrorism, subversion and legitimate dissent and protest’ has taken place during the last decade (Home Office, 2009: 78). In an administrative context, Local Government Authorities, the police, and private sector interests have been aligned under the Civil Contingencies programme to form Local Resilience Forums, which coordinate regional efforts to prevent serious incidents. The possible events cited as having a detrimental impact on vital public services, commercial businesses, or on the general population, include industrial accidents, outbreaks of human or animal-borne disease, and even severe weather. While, arguably, the LRFs are contingency planning centres for predicting and managing risks to each catchment of the UK, they are neither intelligence agencies (on the scale of the DHS), nor do they undertake covert infiltration operations. As civil contingency partnerships, they do however, coordinate with the police (and by extension, with organisations such as the security service MI5, and GCHQ), and they do list public protests as posing threat to public safety. In this respect, the LRFs disseminate MIE discourse into the public domain in relation to the specific sites under their protection (such as power stations and airports). These risks are openly published in Regional Risk Registers and contribute to a National Risk Register which is accessible online.

Evidence to corroborate the allegations outlined above, was first highlighted in an article entitled 'How police rebranded lawful protest as 'domestic extremism'’, by journalists from the *Guardian* newspaper (2009: 6). Here, Evans, Lewis, and Taylor reported that MIE descriptors had become one of the constabulary’s main techniques for legitimising surveillance during public order actions. They noted that MIE terms including domestic extremism were being used in an attempt to undermine public support for causes such as environmentalism, and had led to the details of several thousand suspected extremists being stored on a secret police database (*Ibid*). According to the *Guardian*, evidence that official sources were using domestic extremism as a means to defame campaigners, had been found in an operational review of the public order action at Drax Power Station in 2006. Although initial requests to police sources offered limited results, a Freedom of Information request targeted at North Yorkshire’s LRF, provided evidence of an MIE being used during the police operation. In this respect, a good working knowledge of the systems, policies, and agencies that one is trying to research, will often lead to creative alternatives if the direct approach does not work. In the above instance, an FOI request could have been submitted to the fire brigade, the ambulance service, or to North Yorkshire County Council, where police or state censorship might have been less obstructive. The problem for academics and journalists is that when legitimate protests become aligned with mass-casualty terrorism, they become a matter of national security and not domestic policing. It is the alignment of national security matters with those of domestic policing that makes researching the deep state even more problematic.

While the UK’s LRFs represent contingency planning forums, intelligence-led activities are more conventionally conducted by the police, sometimes by private security firms or by corporate spies (Lubbers, 2012), or by the UK’s security services. Overall, the British equivalent of a fusion intelligence complex is just as adverse to public scrutiny, and is equally as difficult to research as its overseas allies. Nonetheless, the intelligence infrastructure of the UK can really be broken down into three parts. One of these can be thought of in terms of conventional policing (via HM Constabulary), the second as Britain’s intelligence agencies (GCHQ, MI5, and MI6), while the third is military intelligence.[[3]](#endnote-3) Whereas MI6 (the Secret Intelligence Service) is largely responsible for conducting overseas operations, MI5 directs Intelligence operations at home. GCHQ is the UK’s signals intelligence (SIGINT) provider, and alongside its fusion intelligence complex (the Joint Threat Analysis Centre), distributes various information streams to more conventional partners such as the Counter Terrorism Command unit at London’s Metropolitan Police.

Within the Metropolitan Police Service, Counter Terrorism Command (also known also as Special Operations Group 15, or SO15), forms part of the Nation’s wider network of similar organisations. SO15 is the lead branch on counter-terrorism duties in the UK and, according to the sub-divisional North East Counter Terrorism Network, represents just one in a federation of five such institutions […] Overall the Counter Terrorism Network is responsible for intelligence gathering activities and preventing ‘incidents of terrorism and domestic extremism’ […] The five partners report their findings back to Counter Terrorism Command, and thereafter to the Joint Terrorism Analysis Centre, thus forming a network of major regional forces and their respective subdivisions. (Harbisher, 2015: 478)

Although the paradigm set out above demonstrates how the British fusion intelligence complex is currently comprised, as is the case with Monahan (*et al’s*) work in this field, it is worth considering the development of these institutions and the rise of an MIE discourse in the UK as a justification for public order surveillance. In actuality, the majority of information presented so far has been achieved by networking with journalists, by submitting Freedom of Information requests, and also by consulting official publications. Wider approaches to deconstructing the intelligence apparatuses of the British deep state can be found by performing an analysis of publications from other Government Departments, which may work with these organisations. In terms of the alignment of political activism with international terrorism, a good starting point for any investigation is to look at the multitude of official publications on terrorism, and then by cross-referencing the institutions involved (including those cited as contributors).

In terms of understanding the origins of MIE discourse in the UK, a number of initial publications made reference to an organisation known as the RICU. The Research Information and Communications office at Whitehall is essentially a think tank that operates between three separate departments. These are the Foreign and Commonwealth Affairs Office, the UK Home Office, and the Department for Communities and Local Government. The RICU was established in 2007 and promotes consistent communication strategies between CONTEST stakeholders and the general public. Under the PREVENT strand of CONTEST (designed to tackle the causes of terrorism and radicalisation at their roots), the RICU aimed to create an alternative narrative to brands such as al Qaeda. Instead of disseminating messages into the public domain that legitimise radicalisation, the RICU encourages all public-facing agencies to use a strategic dialogue in their communications (RICU, 2010). For example, the RICU urges all CONTEST partners not to use terms such as ‘Jihad’ in their communications, as this ‘feeds the idea that there is a religious war between ‘Muslims and the West.’’ (*Ibid*: 58). It claims that using terms such as ‘violent extremism’ offers credible alternatives to depicting terrorists as promoting a specific cause, and in this way, aims to challenge the language of terrorism (*Ibid*: 66).

However, there is limited differentiation in the popular imaginary between a violent extremist and a domestic one. This later proposition illustrates the potency of MIE discourse in the West, especially when used as a political vehicle to restrict freedom of speech and freedom of assembly. The problem is that organisations such as ACPO-TAM and the police, use an equivalent MIE discourse to define campaigners, as that used to describe acts of mass-casualty terrorism. Again, knowing the institutions involved, a wider internet search for key terms such as “ACPO”, “terrorism”, and “language table”, revealed a publication disclosed under the Levenson enquiry entitled *Guidance on Media Handling and Communication Activity at Major Incidents (Including Counter Terrorism)*, authored by ACPO in 2008 for British Transport Police. The document contains precisely the same language table as issued by the RICU, and (knowing that the acronym of “TAM” stands for terrorism and allied matters), it is therefore possible to understand how ACPO subsidiary the NPOIU would have depicted campaign groups as domestic extremists.

**Conclusion: Issues and Problems in Researching the Deep State**

The biggest issue facing journalists or academics conducting research into the politics and practices of the deep state are generally all access-related. On the one hand, FOI requests offer a legitimate way to conduct research in this field yet, comparatively, significant proportions of the material which may (or may not) be returned will be suppressed as a result of National Security censorship. In fact, the UK *Freedom of Information Act* makes explicit reference to materials that will be redacted for the purposes of National Security (*Freedom of Information Act* 2000, Part 2: S24). Often researchers will be faced with several pages that are completely obscured. However, conducting shrewd investigations into the subject matter of interest, allows researchers to read between the lines and to be more selective in their choice of evidence. For example, a public disclosure into the activities of the Special Demonstration Squad (an earlier incarnation of the NPOIU), revealed that undercover officers were advised to have ‘fleeting, disastrous relationships with individuals who are not important to your sources of information’ (Metropolitan Police, 2015: 8). While Operation Hearne (HM Constabulary’s own investigation into allegations that undercover officers had maintained personal relationships as part of their cover), was considered a breakthrough in terms of open government access, no less than 42 pages out of the 52 page disclosure were redacted. With the exception of the above citation (which was of substantial interest to journalists), the rest of the material was unusable.

But there are other problems presented in using FOI/ATIA data sets. Previous searches for evidence (that may have produced usable results), can also be rescinded and removed from public access entirely. Fortunately, online campaign groups (and research foundations) such as Powerbase and the Undercover Research Group, now store previously accessed materials, formerly used by journalists, academics, and activists, that are no longer available in the public domain. Many such documents are today released by the authorities for a limited time only (perhaps due to storage issues), but frequently to limit general public access. In other respects, where criminal cases have been reopened or an inquiry has been called for, evidence may become unavailable in relation to forthcoming trials or police investigations. Nevertheless, as noted by Monaghan and Walby:

The depths of information accessed through the ATIA can be remarkable, yet researchers continue to encounter stonewalling [...] Due to redactions, delays, as well as problems such as chronic under-funding of ATI branches […] ATIA users are aware that these requests rarely lead to full-picture explanations. However, disclosures can be combined to reveal policing and intelligence trends. ATI requests also allow a way of collecting data when it is not possible to conduct interviews. (2012: 138)

There are of course further limitations in using FOI data requests in the UK. In terms of stonewalling, HM Constabulary operates a Neither Confirm Nor Deny (NCND) policy for sensitive issues or publications. As noted above, FOI requests can be delayed if the appropriate operational codename is not used in the first place. In fact it is always advisable to seek an alternative method (such as an LRF request), to provide the basic outline and parameters for your research. Even knowing the key times, dates, operational names etc. of the event in question can be beneficial to this process. Other barriers to legitimate FOI research can include fees being charged by public authorities to pay for the administrative time that an FOI will allegedly take. However, policies that do not even provide an opportunity for further research, like the ‘Neither Confirm Nor Deny’ approach applied to crucial policing events is just as obstructive as it sounds.

There are of course, other avenues for research. The use of data sets provided by whistle-blowers sometimes fills in many of the areas left blank by FOI censorship, although these sites are allegedly monitored by GCHQ and its subsidiaries (Greenwald and Gallagher, 2014). Furthermore, many influential figures involved with investigating the deep state (Duncan Campbell, and Glen Greenwald especially), have themselves been the subject of police intimidation on a number of occasions. Campbell for instance has stated that:

In my 40 years of reporting on mass surveillance, I have been raided three times; jailed once; had television programs I made or assisted making banned from airing under government pressure five times; seen tapes seized; faced being shoved out of a helicopter; had my phone tapped for at least a decade; and […] been lined up to face up to 30 years imprisonment for alleged violations of secrecy laws. (2015)

For figures such as Edward Snowden and Julian Assange, whose leaks have revolutionised the way in which the general public now understands its relationship with the state, the price paid for investigating, or for disclosing deep state secrets, has been even higher. Snowden for example, is currently in asylum in Russia, and has been there since 2013, for fear that his return to the United States would not result in a fair trial. Julian Assange (founder of the WikiLeaks project) is currently under asylum in the Ecuadorian Embassy in London, where he has been since 2012. Journalist Glenn Greenwald and documentary filmmaker Laura Poitras have either been held at Airports during terrorism-related investigations, or have had their immediate family/partners intimidated in this manner for their respective roles in the Snowden affair (Maas, 2013).

It could be suggested than, that conducting investigations at a local or regional level generates less interest from the authorities than stirring the metaphorical hornet’s nest of multinational and government concerns. That said, without the tireless efforts of journalists such as Duncan Campbell, Glenn Greenwald, Rob Evans, Paul Lewis, and Matthew Taylor (*et al*), both civil liberties and contemporary reportage in this area would fare much less well. Comparatively, significant amounts of data regarding the techniques and technologies of the deep state would remain entirely hidden without whistle-blowers such as Edward Snowden and Julian Assange, though they play a precarious game of cat and mouse, caught between their own ethical challenges, and the contentious practices of the state.

**References**

ACPO. 2008**.** *Guidance on Media Handling and Communication Activity at Major Incidents (Including Counter Terrorism)*. London: ACPO.

Anglesey County Council. 2007. ‘Emergencies’. *Anglesey County Council*. Available online at: http://www.anglesey.gov.uk/doc.asp?cat=3370 [Accessed 05 January 2007].

Brown, Jonathan. 2006. ‘The Battle of Drax: 38 held as protest fails to close plant’. *The Independent*. 1 September 2006.

Campbell, Duncan. 1976. ‘The Eavesdroppers’. *Time Out*. May 21-27, 1976: 8-9.

Campbell, Duncan . 1988. ‘Somebody’s Listening’. *New Statesman*. 12 August, 1988: 10-12.

Campbell, Duncan. 2015. ‘GCHQ and Me: My Life Unmasking British Eavesdroppers’. *The Intercept*. Available online at: https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/. [Accessed 10 December 2016].

City of London Police. 2011. *Terrorism/ Extremism Update for the City of London Business Community: 2 December 2011.*London: City of London Police.

DHS. 2016. ‘Fusion Center Locations and Contact Information’. *Department for Homeland Security*. Available online at: https://www.dhs.gov/fusion-center-locations-and-contact-information. [Accessed 10 December 2016].

Evans, Rob. Lewis, Paul. and Taylor, Matthew. 2009. 'How police rebranded lawful protest as 'domestic extremism'’. *The Guardian*, 26th October 2009: 6.

Evans, Rob., and Lewis, Paul. 2013. *Undercover*. London: Guardian Books.

Greenwald, G. 2013. ‘NSA Prism program taps in to user data of Apple, Google and others’. *Guardian*. Available Online at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. [Accessed 05 September 2010].

Greenwald, Glenn., and Gallagher, Ryan. 2013. ‘Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters’. *The Intercept*. Available Online at: https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/. [Accessed 05 September 2010].

Harbisher, Ben. 2015. ‘Unthinking Extremism: Radicalising Narratives that Legitimise Surveillance’. *Surveillance and Society*. 13 (3/4), 474-486.

HMSO. 2000. *Freedom of Information Act* 2000. London: Her Majesty’s Stationary Office.

IPCC. 2011. *Ratcliffe-on-Soar Power Station (Operation Aeroscope) Disclosure: Nottinghamshire Police*. Sale: Independent Police Complaints Commission.

Jones, Chris. 2014. “Call it intercontinental collaboration”: radicalisation, violent extremism and fusion centres. *Statewatch*. London: *Statewatch.*

Jones, Meirion. 2011. ‘Trial collapses after undercover officer changes sides’. *BBC Newsnight*. Available Online at: http://www.bbc.co.uk/news/uk-12148753. [Accessed 10 October 2016].

Lubbers, Eveline. 2012. *Secret Manoeuvres in the Dark: Corporate and Police Spying on Activists*. London: Pluto Press.

MacAskill, Ewel., Borger, Julian., Hopkins, Nick., Davies, Nick., and Ball, James. 2013. ‘GCHQ taps fibre-optic cables for secret access to world's communications’. *Guardian*. Available Online at:

https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. [Accessed 05 September 2010].

Maas, Peter. 2013. ’How Laura Poitra Helped Snowden Spill his Secrets’. New York Times. Available Online at: http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html?pagewanted=all&\_r=0. [Accessed 10 October 2016].

Metropolitan Police. 2015. *Operation Hearne – SDS Tradecraft Manual*. London: Metropolitan Police.

Monahan, Torin., and Palmer, Neal. 2009. ‘The Emerging Politics of DHS Fusion Centres’. *Security Dialogue.* Vol. 40*,* no. 6: 617-636.

Monahan, Torin. 2009. ‘The Murky World of 'Fusion Centres'’. *Criminal Justice Matters* 75 (1): 20 — 21.

Monahan, Torin. 2010. The Future of Security? Surveillance Operations at Homeland Security Fusion Centres. *Social Justice.* Vol. 37, Nos. 2–3: 84-98.

Monaghan, Jeffrey., and Walby, Kevin. 2012. ‘Making up ‘Terror Identities’: security intelligence, Canada's Integrated Threat Assessment Centre and social movement suppression’. *Policing and Society: An International Journal of Research and Policy*, 22:2, 133-151

Newkirk, Anthony. 2010. ‘The Rise of the Fusion-Intelligence Complex: A critique of political surveillance after 9/11’. *Surveillance & Society* 8(1): 43-60.

North East Counter Terrorism Unit. 2015. ‘Background’. Available Online at: http://www.northeastctu.police.uk/about/background. [Accessed 01/04/2015].

North Yorkshire Local Resilience Forum. 2006. *North Yorkshire Local Resilience Forum: Notes of the Joint Operations Group*. Northhallerton: North Yorkshire Local Resilience Forum.

RICU. 2010. *Prevent: A Communications Guide*. London: Home Office.

Rose, Christopher. 2011. *Ratcliffe-on-Soar Power Station Protest Inquiry into Disclosure*. London: Crown Prosecution Service.

Shubber, Kadhim. 2013. ‘A simple guide to the Prism controversy’. *Wired*. Available Online at:

http://www.wired.co.uk/article/simple-guide-to-prism. [Accessed 05 September 2010].

TSO. 2009. *Security for the Next Generation*. London: The Stationary Office.

Wilson, Eric. 2009. *Government of the Shadows: Parapolitics and Criminal Sovereignty*. London: Pluto Press

1. The ACPO was officially formed in 1948, but was later turned into a limited company to restrict public access to records under Freedom of Information requests in 1997. ACPO was formally disbanded in 2015 and re-emerged as the National Police Chief’s Council. [↑](#endnote-ref-1)
2. Including the *Vancouver Sun*, *Toronto Star*, and the *Ottawa Citizen.* [↑](#endnote-ref-2)
3. The lineage of GCHQ, MI5 and MI6 stems from the designation of military codenames during World War Two. GCHQ in particular hails from the code breakers and cyphers division of Bletchley park fame, and deciphered the German Enigma device during the conflict. [↑](#endnote-ref-3)