Social Networks for Surveillance and Security:
'Using Online Techniques to make something happen in the real or cyber world'

Ben Harbisher

Abstract
This chapter examines the use of Social Networks for Surveillance and Security in relation to the deployment of intelligence resources in the UK. The chapter documents the rise of Military Intelligence agencies during both World Wars (such as GCHQ and MI5), and the subsequent use of these institutions to maintain order during peacetime. In addition to the way in which military organisations have used clandestine techniques such as double agents, spies, and various programmes designed for conducting Signals Intelligence, the Chapter offers an insight into how contemporary modes of communication (via mobile devices and the internet), shape the way in which intelligence agencies now gather information. The chapter also considers how the UK's intelligence community responds to National Security issues such as international terror attacks, and how additional threats such as political subversion are framed in National Security discourse as being the legitimising factors behind mass surveillance. Thereafter, the chapter examines how online techniques are used by Britain's intelligence agencies to maintain National Security, and how counter-intelligence strategies are being turned against the population to encourage political compliance. The chapter examines how online espionage techniques for entrapment, coercion, and misdirection, are being used to make something happen in the real or digital world.

Introduction
One of the most prominent threats posed to civilian populations and to the modern nation state today, can be considered in terms of attacks being conducted through digital worldwide networks. As opposed to traditional forms of munitions-based warfare and organised crimes, the unprecedented growth of digital communication platforms and social media has posed a number of challenges to security providers and to private citizens alike. Modern risks presented by the widespread use of digital networks includes hacking and data/identity theft and other forms of cybercrime; the relatively new vogue in cyber warfare (such as techniques to disable the communication systems of hostile or unstable regimes); and in terms of espionage, the manipulation of online content for the

purposes of disseminating propaganda and disinformation to influence the behaviour of specified targets.

The purpose of this chapter is to examine the conspicuous alignment of military and civilian programmes in surveillance, in relation to the securitization of social media networks and cyberspace. The chapter investigates a range of Signals Intelligence (SIGINT) protocols and the institutions who implement them, and explores the deployment of SIGINT operations against non-military targets such as the perpetrators of serious organised crimes and political activists in the UK. The chapter considers how online social networks have become an invaluable tool for maintaining national security, focusing on the agencies who conduct both mass and targeted forms of surveillance through this particular medium. The purpose of this research is to define which modern agencies are responsible for providing Signals Intelligence, and the uses to which this material is put. Here it is the aim to discuss two SIGINT strands in particular, by focusing on Britain's Counter-Intelligence and Effects capabilities. In this respect, Counter-Intelligence Programmes (known as COINTELPROs) exploit Signals Intelligence for the purposes of conducting covert actions against strategically valuable targets to the UK. The SIGINT capabilities of COINTEL agencies are defined by the way in which modern communications systems can be infiltrated and exploited to disrupt the activities of both terrorists and criminal organisations. In terms of Operational Effects, the intention of this subterfuge is to employ a range of online techniques to have an impact on recipients in the real world – ideally before any police coercion or military interventions are required. Security agencies today are able to infiltrate private chat rooms to monitor discussions, post online content to dissuade deviant actors from either planning or enacting their crimes, and even plant materials to discredit the reputation of key suspects during an operation.

However, to problematize the issue of conducting online surveillance to regulate social networks, the techniques used during SIGINT and COINTELPRO operations have in recent years been employed to subvert legitimate social movements in the UK. Evidence from a range of sources suggests that SIGINT and COMINT (Communications Intelligence) resources have been used to discredit non-military targets as well as volatile overseas regimes. Indeed such protocols have allegedly been used for maintaining public order in addition to fighting serious organized crimes and terrorism, that is, by gathering intelligence of public demonstrations and disrupting the communications systems of those involved (Occupy London, 2015). In terms of open democracy, these clandestine practices pose a very serious threat to both civil liberties and human rights in the UK, just as much as they contravene the legitimate right of citizens to conduct peaceful

demonstrations. A bigger question then, transpires in relation to the ultimate objective of such programmes. On the one hand, COINTELPRO activities may seek to pre-empt costly public order operations, yet, in another respect, does the state have the right to modify the behaviour or the opinions of activists - especially when such organisations may seek to campaign against unpopular or unfair policy decisions? What really it boils down to is a question of framing. In other words, of how intelligence organisations depict legitimate acts of dissent as threats to national security, and what the response of such agencies might be to these risks.

Code Breakers and Spies – From National Defence to National Security

The UK's National Intelligence Machinery can be divided into three categories, and the historical emergence of these organisations is important to observe. Principally, they can be defined as Military Intelligence, National Security agencies, and the traditional police authorities of England and Wales. Arguably, in today's intelligence market, these three institutions (and their many subdivisions) often share intelligence resources and a number of operational procedures for keeping citizens safe from harm. Government Communication Headquarters (GCHQ) for example, is responsible for gathering Signals Intelligence, and for disseminating this data to relevant parties. SIS/MI6 is the UK's Secret Intelligence Service and generally operates overseas to monitor persons or regimes of interest. Comparatively, MI5 is the UK's National Security Service and deals ostensibly with domestic matters (i.e.; internal threats posed to Parliamentary Democracy via subversion, by terror attacks, and from other forms of serious organised crime). Lastly, HM Constabulary represents a full-time permanent police force that patrols Britain's streets to prevent or detect crimes, and is otherwise used to maintain public order. Nevertheless, all of the above now works in unison in response to serious threats posed to National Security by terrorist organisations, and from designated groups intending to commit terror-type attacks against the UK (Cabinet Office, 2008: 4).

With the exception of HM Constabulary (whose legislative origin dates back to the *Metropolitan Police Act 1829*), the other institutions mentioned above are relative newcomers to matters of National Security. During the Nineteenth Century for example, the *Metropolitan Police Act* effectively formalised a number of different provincial watch services in the London area for the purpose of creating one unified police force. By 1839 the majority of independent watch services (such as the river police, mounted and pedestrian patrols), were unified to form the Metropolitan Police Force. Elsewhere in the UK, local parish and mu-

nicipal policing services were formalised by the late 1860's, and were organised into local and regional divisions - with the exception of the Metropolitan Police Service and the City of London Police. Today, the Metropolitan Police Service manages the greater London area, and the City of London Police patrols London's financial district. The rest of HM Constabulary is broken down into regional administrative divisions and into the subsequent law enforcement agencies they manage in each district or town.

In terms of Military Intelligence, the majority of agencies now used to conduct espionage, surveillance, and counter-intelligence activities in the UK, began life during the early Twentieth Century. In 1909 the Secret Service Bureau commenced operations following requests made by the Admiralty and the War Office to monitor the Imperial German Navy (which was considered a substantial threat to the British Empire). According to military historian Christopher Andrew, the 'Secret Service Bureau got off to a confused start', with the appointment of two sufficiently experienced officers in the field of navel and military intelligence - neither of whom had been given much of an explanation as to what their particular roles might involve (2010: 25). As a result of this administrative gaffe, Captain Vernon Kell and Commander Mansfield Cumming decided between them, that it would be best to divide their responsibilities according to foreign and domestic intelligence affairs. Kell would gain oversight of naval and military intelligence at home, whereas Cumming's portfolio would govern equivalent operations overseas. It was this division of roles that later compelled the Secret Service Bureau to become two separate organisations.

As early as 1910, the distinction between the two intelligence agencies was already apparent in Whitehall, but it was agreed that both offices would continue to operate as the Secret Service Bureau. By the outbreak of World War One, the Bureau had formalised its overseas operations under the codename of the Special Intelligence Service (SIS), although it was officially recognised as part of the Directorate of Military Operations, MI1(c). SIS was responsible for establishing a network of spies either within the borders of Imperial Germany (which it did with limited success), or more effectively in the German Empire's neighbouring countries of Belgium, Russia, and France (Lerner, 2017). The domestic activities of the Bureau, however, had a lot more impact during this formative period - which was to conduct counter-espionage activities in the UK. Kell's group of operatives was commissioned to work under Section 5 of the Directorate of Military Operations group MO5(g), which, following the reconfiguration of the Directorate in 1916, became unofficially known as MI5 under the Directorate of Military Intelligence.

The MO5(g) was formally established by the Secret Service Bureau during this period, and by 1914 it was already conducting counter-intelligence operations against German spies on British soil. MI5's early accomplishments came from a pre-emptive strike against suspected foreign agents just as the Declaration of War was being announced. Working with MO5(g), Special Branch officers from Scotland Yard arrested 22 German spies as soon as the declaration was made on August 4, 1914. The Bureau later claimed that this nationwide campaign had removed the majority of German spies from British soil, and had given the UK the strategic edge in the forthcoming conflict. By 1917, MI5 (as it had become known) had accumulated a list of all foreign aliens living or working in the UK, and had processed the entrants according to the military risk they posed (Andrew, 2010: 58). At this time MI5's main resource (known as the Central Registry) contained over 27,000 records of individuals who the organisation held under suspicion for one reason or another. This colossal archive had been assembled in-part from communication interception orders through which the postal mail of suspected foreign agents had been seized and then scrutinized. Although officially disputed by the Post Office, these interception orders were upheld by former Home Secretary, Winston Churchill by way of Home Office Warrants to confiscate any incriminating evidence (*Ibid*: 37).

As a result of its initial successes MI5 ventured into more political territory during the Great War, beyond its initial role as the UK's foremost counter-espionage organisation. In addition to hunting for foreign spies who were working in the UK, MI5 expanded its activities to conduct investigations into anything that might hamper the war effort. This included anti-conscription and pacifism groups who opposed the war, and also (as a means to occupy its expanding body of agents) to monitor Britain's Trade Labour movement as well. It was feared that industrial unrest provoked by the trade unions would cause the manufacture of weapons and munitions to cease, and that such organisations were vulnerable to infiltration by foreign agents who would incite dissent. However, despite its initial gains, following the First World War MI5 was subjected to nearly twenty years of executive scrutiny, administrative oversight, staffing and funding cuts, by consecutive peacetime governments. Although MI5 had flourished during the Great War, the scale of its operations, the number of agents it maintained, and the budgetary demands it placed on Whitehall were considered excessive by post-war standards. By late-1919, MI5's activities were curtailed by a reduction in staffing from over eight-hundred operatives to only twelve agents.

Although the activities of MI1(c), the Special Intelligence Service were perhaps less prominent during the Great War (due to the veil of secrecy sur-

rounding such actions), Britain's own attempts at international espionage were a comparative success. According to the organisation itself, significant intelligence was gathered through the use of defectors and informants, and by a network of female spies known as 'La Dame Blanche' (SIS, 2017). At the height of the War, La Dame Blanche was reputed to have over eight hundred operatives working on its behalf in central Europe. The group provided daily reports on the movement of German troops by rail, and were often recruited from the medical professions (as midwives and nurses had permission to cross international borders and military lines). Towards the end of the War, the SIS was awarded control of Room 40, Whitehall's signals and communications division. Room 40 was comprised of Army and Naval intelligence officers, and had deciphered a number of encrypted military and diplomatic codes during the conflict. By 1919, Room 40 was merged with section 1b of Military Intelligence (MI1b), to form the Government Code and Cyphers School (GC&CS) operating under SIS oversight. By the early 1920's the GC&CS had managed to break the far more complicated ciphers used by the Bolshevik Government in Russia, thereby establishing a permanent legacy in British SIGINT history (Lerner, 2017). Yet, the most significant threat of all was entirely overlooked by the SIS during this era. Although the SIS 'uncovered evidence of Nazi-Soviet cooperation in the development of weapons technology', it was entirely unprepared for the German reoccupation of the Rhineland in 1935, preceding the outbreak of the Second World War (*Ibid*).

By the outbreak of war in 1939, MI5 and the SIS were not alone in their efforts to wage clandestine campaigns against threats to British sovereignty. During the second global conflict, the Directorate of Military Intelligence expanded both its activities and its subdivisions exponentially. Between 1939 and 1945, Military Intelligence ran nineteen such groups whose roles varied from undertaking counter-intelligence operations (MI5), debriefing prisoners of war (MI19), conducting the interrogation of escaped prisoners of war (MI9), gathering overseas intelligence (MI6/ the SIS), and directing propaganda campaigns - including the censorship of wartime correspondence (MI7). Prior to the outbreak of war, however, MI5 was considered a dysfunctional outfit despite its earlier success during WW1. This was in-part due to its adherence to out-dated operational paradigms, the sheer diversity of its portfolio of interests, due to power struggles within its leadership, and to a number of perceived failures during the Irish War of Independence. Beyond these issues, it seemed MI5 had been unable to perceive any additional threats to the UK, beyond merely hunting for spies, and according the Directorate, it could not even do that especially well.

The reason for this lapse in executive support was that during the inter-war period, Soviet intelligence services the People's Commissariat of Internal Affairs (NKVD), and the Main Intelligence Directorate (GRU), had established a new network of spies in Britain. The NKVD and the GRU gained a substantial foothold in the UK by recruiting agents directly from the nobility and from prominent public schools (Andrew, 2010: 161-185). MI5 was forced to adapt to these new strategies of recruitment, and upon finding out exactly who the spies were for these organisations, enlisted them to work as double agents instead. MI5's new 'XX' agents would be used to feed disinformation back to the Nazi regime in one of the War's main campaign innovations, the double cross (The National Archives, 2003). It was the strategic use of misdirection tactics and the double cross initiative that led to the successful D-Day landings during the closing stages of the War that brought MI5 back into popular favour.

During WW2 the Government Code and Cyphers School (GC&CS) also became a key player in providing intelligence of the activities of the Nazi War Machine by intercepting important military communications. Since the First World War the GC&CS had been the UK's foremost institution for decoding diplomatic cyphers and encrypted military communications. Based at Bletchley Park near Milton Keynes, the GC&CS was responsible for breaking the German Enigma device during the Second World War, which was largely accountable for orchestrating submarine attacks against allied forces in the Atlantic Ocean. Working alongside American allies under an agreement known as UKUSA (a British/USA intelligence pact which is still in place today) the GC&CS was instrumental in the cryptanalysis of the Enigma coding device, and the later Allied victory during the Battle for the Atlantic. In 1946, the unit was renamed Government Communication Headquarters (GCHQ), and moved its centre of operations to Cheltenham, Gloucester. Here, its activities expanded exponentially in response to the emergence and wholesale popularity of electronic communication devices, and the wider deployment of Signals Intelligence (SIGINT) resources in the West. GCHQ therefore became a central competent in the UK's National Intelligence Machinery.

According to Aldrich (2010: 2), two significant things happened to GCHQ towards the end of the War – mainly between 1943 and 1948. First, beyond the relocation of the GC&CS to Cheltenham and the rebranding the organisation as GCHQ after VJ-Day, a pact was made between Western Allies in the form of a new global SIGINT alliance. Consequently, this agreement was called the Five Eyes (FVEY) project as an amalgamation of SIGINT resources between the UK, the USA, Canada, New Zealand and Australia. It was named after the initial 5 stake-

holders. Second, and more conspicuously perhaps, all mention of SIGINT virtually disappeared from the 'historical landscape' of intelligence programmes after the defeat of the Third Reich, and into the early days of the Cold War (*Ibid*). But this level of secrecy was not to last. In 1976, investigate journalists, Duncan Campbell and Mark Hosenball revealed the all but forgotten existence of GCHQ in an article entitled 'The Eavesdroppers' for *Time Out* magazine (1976: 8-9). Working on research that he had gathered into the UK's secret SIGINT sites (and from leaks provided by former intelligence contractors), Campbell lifted the veil on one of the UK's most secretive enterprises. Putting SIGINT into context, Campbell alleged that the UK and its intelligence allies managed a series of 'listening posts' across the world in places like 'Cyprus, Hong Kong, Singapore, Belize, Oman, St Helena', and elsewhere (*Ibid*). In the UK, Signals Intelligence was captured via sites such as RAF Memwith Hills, RAF Irton Moor, and RAF Morwenstowe in Cornwall. Not only had Campbell revealed the existence of one of the UK's most sensitive intelligence organisations, but he had discovered the sheer scale of an international SIGINT project as well. Later revelations as disclosed first by Campbell, and thereafter by former intelligence contractor and whistle-blower Edward Snowden in 2013, exposed further programmes in mass public surveillance.

This first of these projects operated under the codename of ECHELON, in which the Five Eyes group of nations (see the UKUSA pact and affiliated parties), harvested signals from the majority of telecommunications providers including military targets, business communications, and from domestic sources. Campbell's initial coverage of the story was published by the *New Statesman* in 1988, in which he alleged that GCHQ (now the UK's largest intelligence organisation), was intercepting all forms of telecommunications content. Of course the existence of such a project was vehemently denied by British authorities until 2001, when the European Parliament commissioned an investigation into the alleged 'existence of a global system for the interception of private and commercial communications' (Schmid, 2001). The European Parliament concluded that GCHQ (and the American National Security Agency, the NSA) had been intercepting domestic SIGINT in the world's largest ever surveillance project. However, it was also determined that as the main protagonists were not spying on their own countries, this particular intelligence project was not strictly breaking any laws – despite its utter contempt for personal privacy. In fact the FVEY's nations were exploiting a number of legislative loopholes in human rights doctrine that permitted them to spy on one another's populations, and then share the information gathered with the relevant parties (*Ibid*). The investigation concluded that:

> The Member States are strongly urged to review their own legislation on the operations of the intelligence services to ensure that it is consistent with the fundamental rights laid down in the ECHR and in the case law of the European Court of Human Rights and, if necessary, to adopt appropriate legal provisions. They are called upon to afford all European citizens the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence. Any of their laws which are discriminatory in terms of the surveillance powers granted to the secret services must be repealed. (*Ibid*, 138)

The main findings of the commission considered that the particular types of mass surveillance being conducted had been used 'to intercept, at the very least, private and commercial communications, and not military communications' (*Ibid*, 11). It was established that ECHELON had been carried out a) without the necessary permission or executive oversight required for an intelligence operation of this nature, and b) that it was disproportionate and of questionable legality (for without identifying any specific targets, it was in violation of Article 8 of the European Convention on Human Rights). The commission called for a revision of safeguards to protect European citizens from disproportionate state surveillance, and to ensure that a necessary system of checks and safeguards be established in various EU territories to govern the security services.

However, in 2013 GCHQ became part of another international scandal, when former security contractor Edward Snowden revealed the scope and complexity of two contemporary versions of ECHELON in a monumental exposé leaked to Western news organisations. Snowden alleged that two further projects in mass surveillance had been commissioned by the FVEYs intelligence community (essentially by GCHQ and the NSA), under the operational titles of PRISM and TEMPORA (Shubber, 2013). It was revealed that PRISM and TEMPORA, aimed to gather intelligence from all forms of digital telecommunications streams, including those conducted online, and that data was again being processed without any legal warrant. It was alleged that GCHQ especially, had tapped into the underwater cables carrying SIGINT data between the UK and the United States. This had been done at various access points containing fibre-optic telecommunications lines throughout the UK. As much of the world's internet traffic passes through the UK and under the Atlantic Ocean into the United States, key intelligence sites had intercepted and processed this data. Irrespective of the former ruling of the ECHELON Committee (under Article 8 of the Euro-

pean Convention on Human Rights), mass surveillance was being conducted on an even greater scale.

Following the disclosure of TEMPORA and PRISM by Snowden, the public outcry generated by human rights groups, by privacy advocates, and by the mass media, precipitated a number of investigations into the warrantless mass surveillance that had allegedly taken place. The main issues concerned the accumulation of Bulk Communications Data (BCD), and the second, to the interception of Bulk Personal Datasets (BPD). What this equates to is the collection of all electronic communications data by GCHQ, including the actual content of emails, of text messages, online transactions, social media profiles, internet viewing habits and chat room posts, and to the capacity of GCHQ (or its affiliates) to mine this data to profile the activities, interests, and personal relationships of anyone they deemed suspicious. In terms of the technicalities involved in an operation of this scale, it was alleged that telecommunications and internet providers had been coerced into compliance to provide access to this data, mainly due to threats restricting their legal right to trade. As a result of Snowden's revelations, rights groups Liberty and Privacy International called for a public inquiry into the alleged mass surveillance of the British population.

Following an inquest into TEMPORA headed by the UK Investigatory Powers Tribunal (set up in the wake of the ECHELON scandal during 2000), it was determined that GCHQ had acted illegally for at least seven years between 2007 and 2014, and had caused numerous human rights violations for conducting this form of mass surveillance without a warrant (Bowcott, 2015). The general reaction from British authorities was that even if TEMPORA existed, any intercepted data would have been provided (again) by one of the FVEYs associates, thereby breaking no British laws. As the bulk of the online data in question was theoretically captured beyond Britain's territorial boundaries, this would also be acceptable. However, the Tribunal found that GCHQ had violated Sections 8 and 10 of the European Convention on Human Rights, and that further checks and balances were required to ensure the proportionality and legitimacy of the surveillance being conducted (*bid*). Following the outcome of the Tribunal, Parliament commissioned the *Investigatory Powers Act 2016*, which indeed granted these rights to British intelligence – but only on the grounds that SIGINT activities such as BCD and BPD interceptions would need to be authorised with a Home Office Warrant first. Nonetheless, the *Investigatory Powers Act 2016* retrospectively legalised the human rights violations that had been conducted by British intelligence for the previous seven years.

GCHQ Subdivisions and Capabilities

The question of what all of the above contributes to the use of modern social networks for providing security and surveillance arises from GCHQ's most recent SIGINT innovations under programmes such as TEMPORA. In 2003, the Joint Threat Analysis Centre (JTAC) was established to work alongside MI5 in the pursuit of terrorists and in the prevention of terrorism-related attacks and serious organised crime. The JTAC is provided with intelligence gathered by organisations such as GCHQ, and disseminates material of interest to other security providers including MI5, MI6, and Counter-Terrorism Command at the Metropolitan Police Service. Also within the UK's National Intelligence portfolio, is a little-known organisation working under the management of GCHQ. The Joint Threat Research Intelligence Group (JTRIG) was revealed as part of the disclosures published in 2013 by journalist Glenn Greenwald and by Edward Snowden. Snowden's documents revealed that the JTRIG operates as part of GCHQ's clandestine SIGINT programme and provides a contemporary rendition of MI5's counter-subversion activities as seen during the two global conflicts of the last century.

Essentially, the JTRIG exploits Signals Intelligence provided by GCHQ, though it is also capable of detecting its own targets and for managing its own portfolio of interests. As opposed to working with Covert Human Intelligence Sources (C.H.I.S.), as might be the case for MI5 and MI6, the JTRIG focuses exclusively 'on the cyber domain (computers and the internet), using both open source data and SIGINT' (Harbisher, 2016). In terms of the basic dimension of these activities, the JTRIG has been reputed to conduct SIGINT, COMINT, and COINTELPRO operations, and has ventured into more clandestine territory in terms of directing Human Intelligence (HUMINT) and conducting Psychological Operations (PSYOPS). The purpose of these techniques according to the JTRIG is to 'make something happen in the real or cyber world', or in other words, to produce Operational EFFECTS (Greenwald, 2014a). The JTRIG's Operational EFFECTS programmes can be considered in a number of ways, but principally these include a) the use of persuasive tactics to change a suspect's potential behaviour; b) the infiltration of public, private, and secure networks online to monitor the activities of designated groups; c) where necessary to intervene or plant material to degrade an individual's reputation; and e), to misinform, deceive, or distract their targets using online propaganda. Indeed all of the above pays homage to the origins of British military intelligence. The JTRIG achieves all of the above, through its exploitation of social networks using platforms such as YouTube, Fa-

cebook, private email and chatroom clients, and through its use of False Flag events or news items released via the internet into the public domain.

During 2011, prominent psychologist Dr. Mandeep K. Dhami was seconded to the Human Systems Group, Information Management Department at the Defence Science and Technologies Laboratory (DSTL) at Porton Down. Porton Down is one of the British Army's most sensitive establishments and is used as a research facility into chemical, biological, radiological, and nuclear (CBRN) defence initiatives, and for the associated military application of a range of other issues as well. In March 2011, Dhami published a classified document entitled *Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations*, which documents many of the JTRIGs operational capabilities. Ostensibly, the JTRIG's activities include the use of online techniques to:

> discredit, disrupt, delay, deny, degrade, and deter

the actions of suspects identified by SIGINT operations (Dhami, 2011: 2). How the JTRIG conducts its military and law enforcement actions can be considered as follows, by:

- Uploading YouTube videos containing "persuasive" communications (to discredit, promote distrust, dissuade, deter, delay or disrupt)
- Setting up Facebook groups, forums, blogs and Twitter accounts that encourage and monitor discussion on a topic (to discredit, promote distrust, dissuade, deter, delay or disrupt)
- Establishing online aliases/personalities who support the communications or messages in YouTube videos, Facebook groups, forums, blogs etc.
- Establishing online aliases/personalities who support other aliases
- Sending spoof e-mails and text messages from a fake person or mimicking a real person (to discredit, promote distrust, dissuade, deceive, deter, delay or
- disrupt)
- Providing spoof online resources such as magazines and books that provide inaccurate information (to disrupt, delay, deceive, discredit, promote distrust, dissuade, deter or denigrate/degrade)
- Providing online access to uncensored material (to disrupt)

- Sending instant messages to specific individuals giving them instructions for accessing uncensored websites
- Setting up spoof trade sites (or sellers) that may take a customer's money and/or send customers degraded or spoof products (to deny, disrupt, degrade/denigrate, delay, deceive, discredit, dissuade or deter)
- Interrupting (i.e., filtering, deleting, creating or modifying) communications between real customers and traders (to deny, disrupt, delay, deceive, dissuade or deter)
- Taking over control of online websites (to deny, disrupt, discredit or delay)
- Denial of telephone and computer service (to deny, delay or disrupt)
- Hosting targets' online communications/websites for collecting SIGINT (to disrupt, delay, deter or deny)
- Contacting host websites asking them to remove material (to deny, disrupt, delay, dissuade or deter) (*Ibid*: 9)

In addition to Dhami's account of the JTRIG's activities, leaked intelligence documents from *CBS News*, and *The Intercept* (largely gathered from the Snowden archives), have detailed a number of case studies in which JTRIG EFFECTS Operations have been a success. Of the JTRIG's main subdivisions (the Iran Team, the Serious [Cyber] Crime Team, the Global Team, the Counter-Terrorism Team, the Cyber Coordination and Operations Team, and the Network Defence Team), the organisation is able to cover the majority of contingencies that might arise online.

For example during 2011, the Global Team was "monitoring" both the impending regime change in Zimbabwe 'by discrediting the present regime', and it was also 'preventing Argentina from taking over the Falkland Islands by conducting online HUMINT' (*Ibid*: 8). The JTRIG's latter operation included posting online content to dissuade Argentinian voters from supporting their government's intentions to reclaim the Falkland Islands under Argentine sovereignty. The Serious [Cyber] Crime Team was using EFFECTS protocols to reduce consumer's trust in both 'front companies' and those selling counterfeit online goods (*Ibid*). The Cyber Coordination and Operations team, was comparatively investigating 'cybercrime and electronic attack[s] by: (1) denying, deterring or dissuading criminals, state actors and hacktivists; (2) providing intelligence for judicial outcomes; and (3) discrediting cybercrime forums and their users' (*Ibid*). However, in relation to potential infringements on freedom of speech (especially those

cited under article 10 of the ECHR - the right to freedom of speech), in 2011 the Serious [Cyber] Crime Team was involved with monitoring 'domestic extremist groups' and other potential threats to Parliamentary Democracy and public safety in the UK (*Ibid*: 9). The following section of this chapter, examines how some of these techniques have been used to prevent serious organised crime, and as a means to maintain public order.

JTRIG COINTELPROs

To briefly put the JTRIG's Operational EFFECTS into some form of context, a directory of tools used by this organisation was published online via *The Intercept* in 2014. The dossier included screen shots of the catalogue of tools that JTRIG agents are able to deploy in any given scenario. These include EFFECTS programmes such as Angry Pirate, Rolling Thunder, and Vipers Tongue, and a series of tools used in the forensic investigation of remotely accessed computers. Angry Pirate for example, is reputed to 'disable a targets account on a computer', whereas Rolling Thunder can be used to conduct a distributed denial of service (DDoS) assault, which is generally deployed to take a website offline (*The Intercept*, 2014). Comparatively, the Vipers Tongue EFFECTS programme is used to prevent calls being made or received by satellite and GSM mobile phones. Packages such as SNOOPY and BEARSCAPE are respectively used to replicate data sets from mobile phones and to plunder the handsets for Wi-Fi connection history.

In relation to known instances in which EFFECTS programmes have been used by the JTRIG, Hacktivist groups such as Anonymous have proven to be a viable target against which to test some of these systems. During Operation Payback in 2011 for example, the JTRIG used HUMINT techniques to coerce one such Hacktivist into divulging his haul of sensitive stolen data from the Federal Bureau of Investigations (Schone, 2014). Here, agents (possibly from JTRIG's Cyber Coordination team) infiltrated an IRC known to be used by Hacktivists, and waited for an individual to start boasting about his antics. When a hacker named p0ke announced that he had stolen the details of over 700 employees from a government website, the agent asked if he had seen a BBC website entitled 'Who loves the hacktivists'. The website was a snare designed to track internet traffic to the page, and this was used to trace p0ke's IP address - leading to a conviction.

> When p0ke clicked on the link […] JTRIG was able to pull up the IP address of the VPN (virtual private network) the hacktivist was using. The VPN was supposed to protect his identity, but GCHQ either hacked into the network, asked the VPN for the hacker's personal information, or

> asked law enforcement in the host nation to request the information. (*Ibid*)

In relation to JTRIG Operational EFFECTS, the purpose of this exercise was to assist law enforcement officials to make an arrest of the suspect, who by his own admission had provided all of the evidence required to make a conviction.

During another 2011 campaign (codenamed Operation Wealth), the JTRIG experimented with a new technical protocol entitled Rolling Thunder. According to the JTRIG, the purpose of Rolling Thunder was to destabilise communications between groups of Hacktivists belonging to the Anonymous collective. In this operation, the JTRIG targeted an Internet Relay Chatroom (IRC) which was being used by 'Anonymous, LulzSec and the Syrian Electronic Army' (Gilbert, 2014). Here, Rolling Thunder was used to launch a coordinated DDoS assault against the IRC, as a means to prevent Hacktivists from organising further attacks on corporate or public sector networks. Ironically, the techniques used by Hacktivists to disable commercial and state websites had been turned against them. Primarily Operation Wealth was intended to provide intelligence to law enforcement agencies of who the key protagonists were in the movement. However, the operation also sought to disrupt one of the group's main communications platforms, thus to highlight the vulnerability of this particular medium to Anonymous. According to journalist Gerry Bello:

> The JTRIG infiltrated chat rooms and other online social spaces used by Anonymous to gain human intelligence on Anonymous members. Once gaining the hacktivist's trust they inserted spyware called Spyeye. This spyware replicated across many computers, converting them into a single remote controllable network entity. (2014)

The above network of bots (remotely accessed computers) was thereafter used to implement the DDoS assault, rendering the IRC utterly useless. In terms of operational EFFECTS, 80% of the users engaged in this forum had abandoned the site one month later according to the JTRIG (Schone, 2014). Nevertheless, according to Bello, the site was also being used by legitimate social movements as well, in terms of providing a secure and (presumably) private space in which to organise public campaigns. Taking the IRC offline potentially caused an infringement of the Human Right to Freedom of Speech for such groups.

Further examples of the particular types of activity that can be accredited to the JTRIG include a number of potential COINTEL and HUMINT operations

(and their EFFECTS) that were conceivably conducted during the Million Mask March in 2015. The Million Mask March has rapidly become an annual event since it first started in 2013; in which campaigners representing a wide variety of social issues converge on various state capitals to demonstrate against state surveillance, government and corporate corruption, austerity measures, financial inequality, and the securitization of the internet. The movement has gained a substantial following, with international demonstrators marching through the streets of major towns and cities every November 5th wearing the now-familiar Guy Fawkes "Guido" masks, synonymous with the Anonymous collective and the dystopian epic, *V for Vendetta*. During the 2015 Million Mask March in London, a number of conspicuous events took place. First the organisers of the event drew attention to a fake Facebook page and to a website that had emerged directing participants to alternative locations for the protest. Then, the website for London's Metropolitan Police Service was taken offline, arguably due a DDoS attack committed by Anonymous. At one point during the protest a police car was also set alight allegedly by demonstrators, though almost immediately the internet was awash with claims that the vehicle was a hoax, or worse still, a plan by the authorities to depict the event as a riot (Harbisher, 2016).

The point is that sometimes it is just enough to provide a distraction from the real events to gain a small margin of success. With regards to online speculation about the "false flag" burning of a police car, it was suggested that the car itself was a propaganda stunt. For several days after the demonstration, the denizens of the internet spent hours looking for evidence that the car was broken-down wreck that had been towed to the site, but of course, promoting these kind of stories keeps people preoccupied and prevents them from getting up to mischief elsewhere online (West, 2015). Indeed those visiting or commenting on such pages can also be tracked in relation to their particular take on events.

Ethical and Legal Considerations

A far bigger question then, relates to the ethical and legal issues posed a) by the net cast by these sweeping forms of mass surveillance, and b) the operational protocols themselves, in so far as they aim (in some cases) to manipulate public opinion on heated political debates, and may change the outcome of policymaking decisions without due consent. With regards to the legislative factors that enable mass surveillance, there are two issues of concern. The first of these issues regards the public exposure of such programmes, is as much as information regarding military and domestic surveillance operations is highly classified, and is

protected as a matter of National Security. The second factor to be considered is the legitimacy of such operations in relation to Human and Civil rights affairs. Of course both of the above issues are intrinsically bound in terms of public policy, under which a number of contingencies are designed to maintain official secrecy. Nevertheless, the question of the legitimacy of state surveillance depends entirely on the population's knowledge of it.

According to The *Investigatory Powers Act 2016*, communications interception warrants (including all forms of digital and telecommunications data transmitted in the UK), can now only be requested by the most senior officials in the security services, in military intelligence, or by the police. These measures are intended to represent a safeguard against the unrestrained and unwarranted use of mass surveillance. However, under the *Investigatory Powers Act 2016*, the number of instances in which social movements can be identified as posing a potential treat, i.e.; to public safety, for preventing outbreaks of disorder, and even for defaming the economic interests of the United Kingdom, indicates that a range of campaign organisations are the potential targets for surveillance. Under the *Act*, the power to grant authorisation for obtaining communications data will usually be given by the Secretary of State providing they meet the following criteria:

> (a) in the interests of national security,
> (b) for the purpose of preventing or detecting crime or of preventing disorder,
> (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,
> (d) in the interests of public safety,
> (e) for the purpose of protecting public health,
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,
> (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,
> (h) to assist investigations into alleged miscarriages of justice,
> (i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—
> (i) to assist in identifying P, or

> (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or
> (j) for the purpose of exercising functions relating to—
> (i) the regulation of financial services and markets, or
> (ii) financial stability. (HMSO, 2016: 51)

Overall, the ethical considerations posed by the *Investigatory Powers Act 2016* would seem to be relatively straightforward, in as much as certain types of surveillance may only be conducted with prior authorisation, and for very particular reasons. However, in terms Human and Civil Rights concerns, what the question really becomes is how are these issues represented or defined in the Act?

In this respect, Section 231 of the *Investigatory Powers Act 2016* focuses on the ethical issue of 'Error reporting', that is, if an operative believes a human right has been violated – then how should this be voiced? The Act states that:

> The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error. (*Ibid*: 187)

Intelligence officers are, therefore, only required to disclose human rights violations (as might be in the public interest for example), providing they do not lead to a lack of confidence in 'national security', to disrupt the 'the prevention or detection of serious crime', prove detrimental to 'the economic well-being of the United Kingdom', or impede 'the continued discharge of the functions of any of the intelligence services' (*Ibid*). Accordingly, this contingency presumes that human rights violations will take place in the future, and prevents the general public from finding out. An addition concern to be cited then, relates to how social movements in the UK, are now framed in National Security policy and in criminal law, to become aligned with the above high risk categories of national security, serious organised crime, public health, and public safety.

Re-defining Terrorism, Subversion, and Dissent

In today's SIGINT market there is perhaps less of an emphasis being placed on Military Intelligence (though make no mistake such institutions collate data from all major communications streams), and a revised focus on detecting new targets for security agencies to track. The main shift from gathering Military Intelligence, to conducting domestic surveillance (or rather, for providing real-time situational awareness of important communications data and events), relates to how the

role of institutions such as MI5 and GCHQ has evolved over the last one-hundred years. Arguably many of these changes took place in secret during the closing stages of the Cold War amidst the collapse of the Soviet Bloc, with a renewed interest being shown in both political subversion and in domestic affairs such as the maintenance of public order. According to Andrew (2010), the expansion of Military Intelligence agencies into conducting domestic surveillance, originally formed part of MI5's attempts to legitimise the growth of the organisation during the Great War. Comparatively, Stella Rimmington (the former Director-General of MI5), has indicated that MI5 has historically maintained an interest in groups who have aimed to subvert British Parliamentary Democracy, demonstrating that the particular types of surveillance used for military purposes have a concise domestic application as well (2001: 161).

During the 1980's especially, MI5 was alleged to have infiltrated the Campaign for Nuclear Disarmament (CND), and was suspected of running a series of smear campaigns in the popular press to discredit the leadership of the National Union of Miner's (Milne, 2004: 307-8). MI5 suspected that the communist party was intending to infiltrate the CND and use it as a front to destabilise the constitutionally elected Government of Margaret Thatcher, and thus posed a threat to National Security. Rimmington has also claimed that the triumvirate of leaders behind the National Union of Miner's (NUM) had openly expressed an intention to destabilise the government, thereby categorising the movement as an immediate target for state surveillance (2001: 163). However, this particular counter-subversion role of MI5 is rather more indicative of its role during peacetime, in which gathering Military Intelligence is substituted for maintaining National Security.

Today, MI5 is responsible to the Home Office, whereas MI6 is responsible to the Foreign Office. Little has changed in this particular context. Nonetheless, following the Cold War, the role of MI5 was somewhat refined, and again this reflects the way in which threats to the UK are now portrayed. In fact the existence of both MI5 and MI6 was only formally recognised by Whitehall in the *Secret Services Act 1989*. Comparatively, law enforcement activities were only included within MI5's operational remits as of 1996. In relation to supporting the police in the pursuit of serious organised crimes, MI5 currently defines its role as being the promotion of National Security against attacks from terrorist organisations, against industrial sabotage and espionage, protecting the UK against foreign states or agents, and 'from actions intended to overthrow parliamentary democracy' (MI5, 2017). It is the above threats to National Security, through

which social movements in the UK have been reclassified as targets for state surveillance, the legitimising factors of which can be found in British law.

Post-9/11 public policy has identified that groups intending to conduct campaigns at designated sites of Critical National importance to the UK (such as power stations and utilities providers, transportation networks and the financial infrastructure), are considered threats to National Security under the UK's Civil Contingencies Programme. Under the *Civil Contingencies Act 2004*, it became an offence to interfere with the commercial operations of such sites, and a range of civil contingencies partnerships were set up to identify key risks to the Critical National Infrastructure (HMSO, 2004). The *Civil Contingencies Act* was originally intended to replace the out-dated *Defence Act 1948* (HMSO, 1948), and the *Emergency Powers Act 1920* (HMSO, 1920). It was considered that existing legislation had failed to cope with events such as the outbreak of foot and mouth disease in 2001 and the nation-wide fuel protests of 2000 - both of which had threatened the provision of crucial domestic services in the UK. The Act was also designed to defend the Critical National Infrastructure of the UK from the threat posed by international terrorist groups committing violent attacks on British soil.

A similar shift occurs in public order discourse at this particular point in history, in which the terminology used to define both terrorists and activists substantially changed. Around 2004, a number of think tanks in the UK and USA started to adopt a new set of descriptors, through which to define terror attacks and those associated with the activities of radical social movements. It was here that terrorists were redefined as violent extremists, and political activists as domestic extremists (Harbisher, 2015). In National Security discourse it was considered that using terms such as 'jihad' legitimised a belief in anti-western values, but again the relationship between defence and security demonstrates how the intelligence community justifies its surveillance of social movements in the UK. As noted by Monaghan and Walby (2012), Jones (2014), and Harbisher (2015), the notion of domestic extremism has gained popularity across the FVEYs intelligence community, and it is used to defame any groups that promote anti-Western sentiments, or who vociferously refute the decisions of Western policy makers. In Monaghan and Walby's work, the Canadian Integrated Threat Assessment Centre (Canada's equivalent of the UK's JTAC), defined campaign groups in opposition to the 2010 Vancouver Olympic Games as an extremist threat (2012: 148). Torin Monahan has also observed that similar threat assessment centres in the United States of America have subjected race orientated groups and student associations to unprecedented levels of surveillance - as they are considered potential hotbeds for extremism (Monahan, 2010: 48).

In the UK, international campaign groups such as the Occupy movement have equally been depicted by the security services as domestic extremists. This technique forms a particular discourse which serves to legitimise how the modern state seeks to control public demonstrations. For example, during the 2011 occupation of the steps outside St Paul's Cathedral, campaigners became aware that their mobile devices had stopped working (Occupy London, 2015). Legal representatives for the group later filed a request under the *Freedom of Information Act 2000*, in an attempt to determine whether or not GCHQ's anti-terrorism capabilities had been used against them to end the demonstration before the 2012 London Olympic Games (RT News, 2015). Of course it is not unusual for Britain's security services to undertake collaborative ventures in this manner. During her work for the DTSL, Mandeep Dhami also alludes to these collaborative partnerships:

> Within GCHQ, the teams work with the relevant Intelligence Production Teams (IPTs) who aid in the initiation and planning of operations based on their analysis of SIGINT… Several teams currently collaborate with other agencies including the SIS, MoD's Technical Information Operations (TIO), the FCO, Security Service, SOCA, UK Borders, HMRC, Metropolitan police, and the National Public Order and Intelligence Unit. (Dhami, 2011: 6)

So not merely is the securitization of cyberspace a question of how modern security agencies define the threats they perceive to British democracy, but in relation to the Operational EFFECTS enacted by groups such as the JTRIG, responses to such issues are conducted using increasingly militaristic techniques that pay homage to the wartime origin of these organisations. The most chilling impact of all is the prospect that on an increasing scale, members of various social movements are becoming aware of what they might say or do online, and how this might be used against them. Recent news reports have indicated that citizens of the democratic West have started to censor their own internet posts for fear of what might happen to them if they openly voice their concerns (Turner, 2016).

Conclusion - Risks and Recommendations

To elaborate on the above problematic, the widespread coverage of state surveillance programmes such as PRISM and TEMPORA in the media, and the documented use of COINTEL procedures against campaigners, has had a number of chilling effects. The first of these (as observed above) relates to the reclassifica-

tion of social movements (such as Occupy and various Environmental groups) as domestic extremists in National Security policy. The second concern is the legitimacy this provides to intelligence agencies to conduct communications surveillance over any groups or individuals they perceive as posing a threat – seemingly with limited consequences for violating their human rights by doing so. Yet, the biggest concern of all is the scant differentiation between legitimate threats and expressions of opinion, which are now determined according to risks posed to the Critical National Infrastructure, or to parliamentary democracy, or in other words - to threats which are not of a terrorist nature. This latter issue frames the conclusion for this Chapter, in as much as for campaigners, there is now significant awareness within these communities of the scope of this surveillance, which is causing them to be cautious in expressing their opinions online.

Recent academic studies have, therefore, attempted to demonstrate precisely how online surveillance has started to shape dissenting public discourse. Stoychef, for example, has typified this concern in an article entitled 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' by suggesting that:

> In today's Internet age, the expression of online opinions leaves digital footprints, inextricably linking individuals to political views they shared weeks, months, and even years prior. In other words, there is a newfound permanency associated with a one-time willingness to speak out online. (2016: 289)

The study provides an analysis of the readiness of the American public to debate key human and civil rights issues on social media, specifically those pertaining to surveillance programmes such as PRISM. The review concluded that whereas '86% of respondents were willing to discuss the Snowden PRISM leak in offline settings […] less than half of those would post about it on Facebook or Twitter (*Ibid*: 299). Indeed for 'the remainder—and majority—of participants, being primed of government surveillance significantly reduced the likelihood of speaking out in hostile opinion climates' such as those found online (*Ibid*).

In other reported cases in which cyber-censorship has had a detrimental impact on freedom of speech, various news agencies throughout the world have concluded that COINTEL Operations are being used in a similar manner. In Belarus for example, state surveillance technology has removed open access to 'particular websites including Facebook' and has enabled 'the creation of fake versions of popular dissident websites' (Taylor, 2013). In South East Asia, Shetty has

observed that Vietnamese activists have 'retreated to the internet' only to discover that 'with invasive surveillance regimes in place and a proliferation of new laws that govern online offences, there are few places left for people to gather, speak or write as they wish' (2016). In the UK, a recent study has also determined that activists are equally aware of the different types of online surveillance in which they participate. According to Ramsay, Ramsay, and Marsden, knowledge of state 'surveillance is largely conditioned by the specific experiences of groups and individuals and by the immediate need to perform successful acts of protest' (2016). In their recent study of public order interventions in the UK, campaigners expressed a greater concern at overt forms of surveillance (i.e.; the use of police cameras and personal searches), and the potential for physical coercion to be enacted during demonstrations, than they did about online surveillance. However, when asked specifically about intelligence organisations such as GCHQ and the JTRIG:

> News of this programme appeared to resonate with activists' direct experiences, such as the sudden appearance of disruptive trolls in online discussions. (2017)

Nonetheless, one of the main observations made by the above was the relatively low levels of security employed by campaigners during public demonstrations in the UK. In relation to the alleged use of COINTEL practices during the Occupy London protests (to disrupt the communications devices of campaigners), there is now a demonstrable need for enhanced levels of security to be used during public campaigns (Occupy London, 2015). According to Lee and Feeney:

> Police often spy on protesters, and the smartphones they carry, and no matter how peaceful the demonstration, there's always a chance that you could get detained or arrested, and your devices could get searched. (*Intercept,* 2017)

Therefore, in a society in which smartphones can be remotely hacked, in which the digital footprint of one's activities remain online, in which secure digital networks get accessed by the state, and in which fundamental human rights seem increasingly at stake, private citizens and campaigners alike should take their privacy far more seriously. This proposition seems increasingly led by privacy groups and by members of the free press, who in the last couple of years have started to promote encryption methods that may well become the norm. Lee and Feeney

especially, are now part of this debate in as much as they offer 'tips on how to prepare your phone before you go to a protest' (*Ibid*). Generally speaking this should be seen as good advice.

References

Aldrich. R. (2010). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency.* London: Harper Press.

Andrew, C. (2012). *The Defence of the Realm*. London: Penguin

Bello, G. (2014, February 6). 'Anonymous revealed to be under attack from both corporate and government spies'. *Free Press*. http://freepress.org/departments/display/20/2014/5336. Cited 02 January 2017

Campbell, D. (1988). 'Somebody's Listening'. *New Statesman*. 12 August, 1988: 10-12

Campbell, D., and Hosenball, M. (1976). 'The Eavesdroppers'. Time Out. May 21-27, 1976: 8-9

Cabinet Office. (2008). *The National Security Strategy of the United Kingdom*. London: Cabinet Office

Dhami, K. (2011). *Behavioural Science Support for JTRIG's (Joint Threat Research and Intelligence Group's) Effects and Online HUMINT Operations*. Porton Down: DTSL

Gilbert, D. (2014, February 5). 'UK government used 'rolling thunder' DDoS attacks against anonymous, LulzSec and Syrian electronic army'. *International Business Times*. http://www.ibtimes.co.uk/uk-government-used-rolling-thunder-ddos-attacks-against-anonymouslulzsec-syrian-electronic-1435186. Cited 02 January 2017

Greenwald, G. (2014a, February 24). 'How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations'. *The Intercept.* https://theintercept.com/2014/02/24/jtrig-manipulation/. Cited 02 January 2017

Greenwald, G. (2014b, July 14). 'JTRIG tools and techniques'. *The Intercept.* Retrieved from https://theintercept.com/document/2014/07/14/jtrig-tools-techniques/. Cited 02 January 2017

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

Harbisher, B. (2016). 'The Million Mask March: Language, legitimacy, and Dissent'. *Critical Discourse Studies*. Volume 13, 2016 - Issue 3: Discourse and Protest Events

HMSO. (2004). *Civil Contingencies Act 2004*. London: Her Majesty's Stationary Office

HMSO. (1948). *Defence Act 1948*. London: Her Majesty's Stationary Office

HMSO. (1920). *Emergency Powers Act 1920*. London: Her Majesty's Stationary Office

HMSO. (2016). *Investigatory Powers Act 2016*. London: Her Majesty's Stationary Office

Jones, C. (2014). "Call it intercontinental collaboration": radicalisation, violent extremism and fusion centres. *Statewatch*. London: Statewatch

Lee, M, and Feeney, L. (2017). 'Cybersecurity for the People – How to Protect-Your Privacy at a Protest'. *Intercept*. https://theintercept.com/2017/04/21/cybersecurity-for-the-people-how-to-protect-your-privacy-at-a-protest/. Cited November 23 2015

Lerner, (2017). 'MI6 (British Secret Intelligence Service)'. *Espionage Information*. http://www.faqs.org/espionage/Lo-Mo/MI6-British-Secret-Intelligence-Service.html. Cited 02 January 2017

Monaghan, J., and Walby, K. (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

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

Occupy London. (2015, November 6). *City Police Questioned on Likely Use of GCHQ's "Anti-Terror" Capabilities during Policing of Occupy London*. Occupy London. http://occupylondon.org.uk/domestic-extremism/. Cited November 23 2015

Ramsay, G., Ramsay, A., and Marsden, S. (2016). 'Impacts of Surveillance on-contemporary British activism'. Opendemocracy. https://www.opendemocracy.net/uk/gilbert-ramsay/report-impacts-of-surveillance-on-contemporary-british-activism. Cited November 23 2015

RT News. (2015). 'Police told to apologize for treating Occupy London protesters as 'extremists'. *RT News*. https://www.rt.com/uk/314846-occupy-london-protest-surveillance/. Cited January 02 2017

Schmid, G. (2001). *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system).* Brussels: European Parliament

Schone, M. (2014, February 14). 'Exclusive: Snowden docs show UK spies attacked anonymous, hackers'. *NBC*. Retrieved from http://www.nbcnews.com/news/investigations/war-anonymousbritish-spies-attacked-hackers-snowden-docs-show-n21361. Cited January 02 2017

Shetty, S. (2016). 'Why is East Asia Silencing Free Speech'. *World Economic Forum*. https://medium.com/world-economic-forum/why-is-east-asia-silencing-free-speech-663726d1b0c8. Cited January 02 2017

Shubber, K. 2013. 'A simple guide to the Prism controversy'. *Wired*. Available Online at: http://www.wired.co.uk/article/simple-guide-to-prism. Cited 05 September 2010

SIS. (2017). *MI6: Our History*. https://www.sis.gov.uk/our-history.html. Cited January 02 2017

The Intercept. (2014). *JTRIG Tools and Techniques*. *The Intercept*. https://theintercept.com/document/2014/07/14/jtrig-tools-techniques/ Cited January 02 2017

The National Archives. (2017). 'Double Cross Agents'. The National Archives. http://www.nationalarchives.gov.uk/releases/2003/may22/doublecross.htm. Cited January 02 2017

Turner, K. (2016). 'Mass surveillance silences minority opinions, according to study'. *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/. Cited January 02 2017

Stoychef, E. (2016). 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring'. *Journalism & Mass Communication Quarterly*. 2016, Vol. 93(2) 296–311

West, M. (2015, November 7). 'Debunked: Cop car towed to media location then torched at Million Mask March – BX10 LNV'. *Metabunk*. https://www.metabunk.org/debunked-copcar-towed-to-media-location-then-torched-at-million-mask-march-bx10-lnv.t6962/ Cited January 02 2017