Outline

DRAFT

About The Wilberforce Society

The Wilberforce Society was founded in 2009 by students at the University of Cambridge. It is the University's student-run think tank, and aims to provide a forum for dialogue between students and leading policymakers.

This core aim is achieved by three key functions: the promotion of public policy debate amongst the wider student body, the publishing of students' policy research to a professional audience, and reaching out to policymakers across the UK to work with students on the formulation of new policy.

For further information on the society, its events and the possibility of commissioning policy research, please visit www.thewilberforcesociety.co.uk or email chairman@wilberforcesociety.co.uk.

Follow @TWSCambridge on Twitter.

Contents

PART I

The Status Quo

Chapter 1

What is the Government Communications Headquarters (GCHQ)?

GCHQ, based in Cheltenham, Gloucestershire, is one element of the broadly tripartite structure of Britain's intelligence community. In contrast to the Security Service (MI5) and the Secret Intelligence Service (SIS / MI6), "GCHQ counters threats that compromise national security through the production of signals intelligence (known as SIGINT) and the security of communications and information systems (known as Information Assurance)".[1] Each of the former are responsible for running operations at home and abroad, potentially acting on information provided by GCHQ.

Currently headed by Sir Iain Lobban, the organisation "works to the Foreign Secretary"[2], which contrasts it with the Security Service, who work to the Home Office, but is comparable to the SIS, whose remit is also international in nature. As with both of these the organisation GCHQ is answerable to Parliament's Intelligence and Security Committee (ISC), created by the Intelligence Services Act 1994, although its activities are directed by the Joint Intelligence Committee (as with all of Britain's intelligence agencies).[3]

Its membership of the Joint Terrorism Analysis Centre (JTAC), which appears to be responsible for co-ordinating Britain's intelligence response to issues including terrorist threats, and providing reports on threat levels, trends and "terrorist capabilities"[4] fits with GCHQ's broader image as the observer in Britain's intelligence set up. Having stated this, GCHQ does seem to have the potential to take a more pro-active stance in relation to cyber-security threats(addressed further under "Where does it operate and what does it do?").

Observation is, however, the key term in relation to GCHQ, and it is in this context that is has been drawn into the public eye following the release of documents pertaining to the NSA and related agencies by Edward Snowden. Sir Iain Lobban insisted during the recent televised

[1] https://www.mi5.gov.uk/careers/working-at-mi5/working-with-mi6-and-gchq/mi5-or-mi6.aspx (11/11/13)
[2] http://www.gchq.gov.uk/who_we_are/Pages/Welcome-to-GCHQ.aspx (11/11/13)
[3] http://isc.independent.gov.uk (11/11/13)
[4] https://www.mi5.gov.uk/home/about-us/who-we-are/organisation/joint-terrorism-analysis-centre.html (11/11/13)

elements of the ISC's first public investigation that the organisation is focused on identifying the small minority of individuals who pose a threat, against the backdrop of wider use. In relation to the broader public the haystack analogy used appears to imply that GCHQ do not spy (in a narrow sense) on the overwhelming majority of British citizens and in fact internet users world wide.[5]

1.1 Where does it operate and what does it do?

Whilst based in Cheltenham GCHQ evidently operates communications surveillance across both the UK and the wider world.[6] The recent allegations of a GCHQ run listening post at Britain's German Embassy would seem to support the suggestion that the organisation is involved in collecting data for defending Britain's interests, in a wider sense than the "What we do" page of the GCHQ website[7] implies, with its focus on the threats faced. Furthermore, it implies a physical geographical extension which is not apparent from the neat division of the services previously attested to. The nature of the world wide web and the international nature of modern communications (going through satellites via cabling and more) and the disparate nature of terrorist organisations such as al-Qaeda mean that GCHQ must collect data originating from beyond the UK's borders.

The accusation raised by "The Independent" that GCHQ has been operating in a UK embassy, in contravention of international law, leaves open the possibility (if true) that this has been repeated elsewhere. It is questionable as to the extent that this differs from intercepting communications from abroad in Cheltenham, and this is the element that most confuses any attempt to identify where GCHQ operates — beyond within the sphere of communication, in particular digital ones.

GCHQ itself divides threats that it engages with into three categories on its website: The cyber threat, The threat from terrorism, Espionage and Serious Crime. In the case of the cyber threat, GCHQ appears to gather data to identify current and potential threats to the UK's industries, as well as working to protect current systems from developing threats. Through giving advice to the Critical National Infrastructure there again appears to be a more active attempt to engage with potential dangers.

What is not readily available is information pertaining to the extent to which GCHQ itself engages in activities of this sort in relation to foreign powers. In light of the Snowden revelations it would seem to be naïve to assume that GCHQ do not engage in more than counter-cyber-espionage activity, but equally the public divides of the UK's intelligence agencies posit a more passive role for the organisation.

The focus on the internet in relation to GCHQ in the media distorts conclusions about its activities, and it is apparent that much of the online observing is focused on the latter two elements. The implication of the short exposition on the website is that GCHQ's primary contribution to

[5] http://www.bbc.co.uk/news/uk-politics-24847399

[6] http://www.independent.co.uk/news/uk/politics/germany-calls-in-britains-ambassador-to-demand-explanation-over-secret-berlin-listening-post-8923082.html (11/11/13)

[7] http://www.gchq.gov.uk/what_we_do/Pages/index.aspx (11/11/13)

thwarting terrorist activities is the monitoring of communications and through the JTAC the distribution of that information to the relevant agencies, including both the Security Service and the SIS. In a similar way the organisation passes "intelligence, capabilities and expertise"[8] on to the National Crime Agency (NCA), helping to address the issue of serious crime.

This domestic element of crime is also to be found in the espionage focus, which is on defending commercial interests as opposed to the more traditional image of Government secrets being the primary concern, the changing technological world has meant that GCHQ appears to be primarily engaged in defending against criminal organisations, as opposed to foreign governments.

The CONTEST Report[9] of earlier this year reveals little of detail regarding specific activities which any of Britain's security services engage in and as a result conclusions must be drawn more generally. This is in keeping with much of the data available through the public websites of relevant organisations. The tendency to generalise makes it difficult to reach any meaningful conclusions regarding GCHQ's activities. With there being little concrete information available there is also a risk of exaggerating what are actually minor elements of their program and of extrapolating patterns of behaviour from isolated examples.

1.2 What are the main threats against which the UK Government deploys intelligence?

From GCHQ it is apparent that there are four broad categories against which intelligence is deployed by the UK government. They are terrorism, espionage (industrial and governmental), serious and organised crime, cyber security. Section 1 of the Intelligence Services Act (ISA) 1994 appears to open up a broad category of potentially valid targets, stating as it does that Britain's intelligence services must work "in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's government in the United Kingdom; or in the interests of the economic wellbeing of the UK; or in the support of the prevention or detection of serious crime"[10]

Claims in the CONTEST 2013 Report reveal that counter-terrorism suggest that intelligence gathering plays a major part in defending the UK from potential attacks and in gathering evidence to be used in court against those charged. Within the spectrum of terrorist threats what is becomes apparent is that the perceived threat from far right extremism is very low, but that despite public perception, the troubles of Northern Ireland continue to be the most common threat to the general public, although more localised.[11] The report makes no causal distinction in relating the statistics on potential attacks. Only marking out Northern Ireland separately and commenting on the risk from the political fringe. As a result, from it and from the wider

[8] http://www.gchq.gov.uk/what_we_do/the-threats-we-face/Pages/The-threats%20from%20espionage-serious-crime.aspx (11/11/13)

[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_Cm_8583_v0_20.pdf (11/11/13)

[10] http://www.theguardian.com/uk/2013/jun/16/laws-intelligence-agencies-spy-foreign (11/11/13)

[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170644/28307_Cm_8583_v0_20.pdf (Sections 1.13 / 1.14) (11/11/13)

data it is difficult to ascertain whether the UK government does focus more on particular subsets of society. Without knowledge of the trigger criteria used by the intelligence agencies this is not something that can be addressed. What can be confidently stated is that intelligence is deployed extensively in combating terrorism domestically. Its use against targets abroad can be assumed, both as a result of the data sharing between, for example, GCHQ and the NSA, relayed by the Snowden breach and as a result of the independent existence of the SIS.

The need to counter-industrial espionage, highlighted by the US government's concerns about the granting of contracts to the Chinese telecoms company Huawei, is explicitly allowed under Section 1 of the ISA (1994). That GCHQ openly admit to working with industry to help secure their data as well as to secure the UK's key infrastructure suggests that intelligence is deployed extensively in preempting threats and, assuming that Britain's intelligence agencies have similar concerns to their foreign equivalents, in the integration of major foreign businesses into the UK markets for certain essentials — communications and energy to name two.

The fall of SilkRoad, the illicit market place for everything from drugs to firearms, has brought the role of intelligence agencies in tackling the problem of organised crime to the fore once more. Efforts by GCHQ and its equivalents clearly do hinder criminal networks and, as in the aforementioned case, can provide essential information to allow the police and others to bring people to justice. The provision of material to the NCA by GCHQ demonstrates the core nature of tackling crime to the security services remit. The NCA itself categorises organised crime into the following sections: "Child sexual exploitation, the latest trends: Cyber crime, Drugs, Fraud, Human trafficking, Intellectual property crime, Kidnap and extortion, Money laundering, Organised acquisition crime, Organised crime groups"[12]

The ubiquitousness of the internet in modern life means that it would seem reasonable to suppose that all of the aforementioned are legitimate targets of the intelligence services — especially the Security Service and GCHQ.

The cyber-security issue to some extent blended with all those previously mentioned. On its own, the key element appears to be in defending the UK's key infrastructure[13] from disruption and in maintaining the UK government's privacy. Inherently defensive in nature, speculatively the intelligence gathered in relation to cyber-security may be of more relevance in compromising the secure communications of organised criminal networks and of terrorist organisations in the UK and abroad.

Abroad the SIS appears to have responsibility in defending Britain's interests and in protecting British nationals through working with foreign intelligence agencies, identifying areas of high risk for travel and neutralising individuals involved in terror and criminal networks world wide. The extent to which data gathered by the SIS influences the success of British companies abroad is particularly difficult to ascertain.

[12] http://www.nationalcrimeagency.gov.uk/crime-threats (11/11/13)
[13] http://www.cpni.gov.uk/about/cni/ (11/11/13)

1.3 References

Centre for the Protection of National Infrastructure Website — www.cpni.gov.uk

Government Communications Headquarters — www.gchq.gov.uk

The Security Service (MI5) — www.mi5.gov.uk

The Secret Intelligence Service (MI6) — www.sis.gov.uk

The National Crime Agency — www.nationalcrimeagency.gov.uk

The Intelligence and Security Committee of Parliament -http://isc.independent.gov.uk

The Guardian — www.guardian.com/uk

The Independent — www.independent.co.uk

BBC — www.bbc.co.uk

A Strong Britain in an Age of Uncertainty: The National Security Strategy

Chapter 2

The Secret Intelligence Service (SIS)

2.1 Origin

Also known by its more popular acronym MI6 (Military Intelligence, Section 6), the British Secret Intelligence Service (SIS) was founded in 1909 in response to the then-present 'spy fever': the fear that German spies had infiltrated the British government services on all levels (Smith, 2011). During its early days, the Service was remarkably small, and after his first day of work, the founding Chief, Commander Mansfield Cumming, noted in his diary: 'went to the office, and remained all day, but saw no one, nor was there anything to do there' (Jefferey, 2010). Over time, the Service has established its reputation as one of the world's most important foreign intelligence services, along with the American CIA and the Russian FSB (the successor of the KGB). The SIS was not formally avowed until 1992, and its role was only codified in 1994 in the Intelligence Services Act (hereafter: the 1994 Act).

2.2 Organisational structure

The SIS is one of the three main British intelligence agencies, together with the domestically oriented Secret Service (also known as MI5) and the Government Communications Headquarters (GCHQ). Its organisational structure was first laid down in the 1994 Act and later revised in the 2013 Justice and Security Act (hereafter: the 2013 Act). SIS is subjected to the Secretary of State and mainly consists of two branches: Production (which deals mostly with obtaining raw information from its sources) and Requirements (which tries to validate the intelligence provided by the Production unit).

2.3 Operations

SIS, as was established in the 1994 Act, has two functions:

1. To obtain and provide information relating to the actions or intentions of persons outside the British Islands; and

2. To perform other tasks relating to the actions or intentions of such persons.

Those functions, however, can only be exercised

1. In the interests of national security (in particular in areas related to defence and foreign policies); or

2. In the interests of the economic well-being of the United Kingdom; or

3. In support of the prevention or detection of serious crime.

Whilst the Service is allowed to obtain intelligence under either of these three circumstances, the Chief is, under Clause 2 of the 1994 Act, only allowed to disclose any information when it is in the interest of national security or in support of prevention or detection of serious crime. Thus, when information is 'only' in the interests of British economic well-being, he is not permitted to disclose it (Intelligence Agencies Act, 1994).

SIS mostly deals with human intelligence (HUMINT), relying heavily on human sources (Davies, 2004). After SIS obtains intelligence from 'raw' sources, the information is subsequently assessed by ministries and departments (Davies, 1995). Thus, as opposed to for example the American CIA, SIS is concerned not so much with analysis but rather with collection of information, and the assessment is viewed as a government function rather than an intelligence function (Herman, 1996).

2.4 Oversight

In the 1994 Act, a Parliamentary Intelligence and Security Committee (ICS) was established, which would oversee the "expenditure, administration and policy" of the three major intelligence agencies: SIS, GCHQ and the Security Service. In the 2013 Act, this oversight capacity was expanded to intelligence-related work of the Cabinet Office. The Committee consists of nine members, each from either the House of Commons or the House of Lords, who are appointed by Parliament and then nominated by the Prime Minister. The ICS can have access to and oversight over a large number of activities of the intelligence services, yet matters that "are part of any ongoing intelligence or security operation" are excluded from their oversight (Justice and Security Act, 2013).

2.5 Critiques

Whilst many acknowledge the importance of the SIS, and the intelligence community in general, a number of critiques have been voiced in recent times. Three of those are most prominent: the first relates to its internal organisation, the second to British organisational culture with regard to intelligence, and the third to the issue of oversight and protection of information.

As was noted, the SIS functions mostly as a 'production' service of intelligence rather than as a service with an analytical function. Since the 1970s, the role of the Requirements department has decreased, allegedly causing a decline in 'quality control' (Davies, 2005). The fact that sources were more relied upon by Production and less scrutinised by Requirements was seen as one of the causes for a number of intelligence failures in situations, ranging from the Falklands War in 1982 to the Invasion in Iraq in 2003. Those failures, as Davies notes, were the result of "inclusion of insufficiently validated subsource reporting" as well as "a failure to adequately lift the intelligence signal out of the background noise and make sure that the signal reached consumers, analysts, and decisionmakers with the required clarity" (Davies, 2005).

Moreover, the focus on production on the part of the intelligence community whilst leaving the assessment role to the government has led to a high degree of "collegiality" within the community (Davies, 2004). The three main intelligence agencies are represented in the Joint Intelligence Committee (JIC), a body that is part of the Cabinet Office and that advises the Prime Minister and the Cabinet on affairs related to intelligence. Within this body, as a former JIC official once noted: "departmental disagreement is felt to represent a collective failure, and formal notes of dissent are rare" (Herman, 1996). This tendency towards committee-wide agreement could lead to groupthink (Davies, 2004).

Lastly, the issue of oversight and protection of information has become increasingly salient, particularly in the discussion of the 2013 Act. On the one hand, there is the issue of 'secret procedures': in both civil and criminal cases, the defendant usually has the right to see the evidence of the other side, but in some cases, the government may decide that the prosecution does not have to reveal information when it can be seen as threatening national security. In the 2013 Act, the government has expanded this 'right to secret procedures', leading to critiques on behalf of civil liberty organisations. On the other hand, there is an increasing public demand for openness of intelligence agencies and government in the wake of the Snowden leaks. How these two developments will play out remains to be seen, but it is certain that the outcome will be important to the way in which intelligence agencies can conduct their operations.

2.6 Bibliography

Davies, P. H. J. (1995). Organisational Politics and the British Intelligence Producer/Consumer Interface. Intelligence and National Security, 10(4), 113–32.

Davies, P. H. J. (2004). Intelligence culture and intelligence failure in Britain and the United States. Cambridge Review of International Affairs, 17(3), 495–520. doi:10.1080/0955757042000298188

Davies, P. H. J. (2005). A Critical Look at Britain's Spy Machinery. Studies in Intelligence, 49(4), 41–54.

Herman, M. (1996). Intelligence Power in Peace and War. Cambridge: Cambridge University Press.

Intelligence Agencies Act (1994). United Kingdom Parliament.

Jefferey, K. (2010). MI6. The History of the Secret Intelligence Service, 1909-1949. London: Bloomsbury.

Justice and Security Act (2013). United Kingdom Parliament.

Smith, M. (2011). Six. The Real James Bonds, 1909-1939. London: Biteback Publishers.

Chapter 3

Which industries are used for intelligence purposes? Which companies are involved, and are there any sectors with only compliant companies?

American telcos are compelled to routinely hand over metadata to the government.

The overall report may need a detailed description of PRISM and XKeyscore.

Two reasons for surveillience: terrorism, since 9/11; and digital revolution

3.1 NSA vs Google, Yahoo: MUSCULAR

- NSA broken into the main communications links that connect Yahoo and Google data centers around the world
- NSA's acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md
- Use MUSCULAR, created with GCHQ
- But both Yahoo and Google deny access has been given to data centres
- Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight where the NSA is allowed to presume that anyone using a foreign data link is a foreigner. FISC has no jurisdiction! ""NSA lawyers, their job to figuring how to stay within the law and maximize collection "

- For the MUSCULAR project, the GCHQ directs all intake into a "buffer" that can hold three to five days of traffic before recycling storage space. From the buffer, custom-built NSA tools unpack and decode the special data formats that the two companies use inside their clouds. Then the data are sent through a series of filters to "select" information the NSA wants and "defeat" what it does not.
- collection from inside Yahoo and Google has produced important intelligence leads against hostile foreign governments that are specified in the documents
- asymmetry in U.S. surveillance law. Although Congress has lifted some restrictions on NSA domestic surveillance on grounds that purely foreign communications sometimes pass over U.S. switches and cables, it has not added restrictions overseas, where American communications or data stores now cross over foreign switches.**key-1**; **key-2**
- Google now encrypted data**key-1**

3.2 NSA vs Facebook, Google, etc. : PRISM

- **key-23**gathers huge volumes of online communications records by legally compelling U.S. technology companies, including Yahoo and Google, to turn over any data that match court-approved search terms
- All major tech companies reject this, who say they only comply with lawful requests for data
- slides http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document #requests per company also availiable

3.3 NSA vs People: XKeyscore

- This NSA spy program captures vast swaths of unencrypted HTTP traffic at secret sites that span the entire world. However, due to storage limitations, it seems that it can only keep that data for relatively short periods of time.

3.4 NSA vs Lavabit

- Ladar Levison, the founder of Lavabit — a small, secure email provider used by Snowden — suspended operations in August rather than comply with a warrant that would have allowed the US government access to the data of all Lavabit's 400,000 customers.

3.5 Encryption Protocols

- Encryption is probably the biggest threat to the NSA and GCHQ.
- NSA, GCHQ can "break" SSL; US agencies have been planing for this for some time.
- Mathematics itself is fine; implementation is poor https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea
- in 2006, the N.S.A. intentionally introduced a vulnerability into an encryption standard adopted by both the National Institute of Standards and Technology and the International Organization for Standardization. http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html
- The N.S.A. also uses its Commercial Solutions Center, which invites companies, including start-ups, to show their technology to the agency under the guise of improving security, in order to "leverage sensitive, cooperative relationships with specific industry partners" and covertly make those products more susceptible to N.S.A.'s surveillance. Schneier, who has reviewed the documents, describes the process thusly: "Basically, the NSA asks companies to subtly change their products in undetectable ways: making the random number generator less random, leaking the key somehow, adding a common exponent to a public-key exchange protocol, and so on." This is why the N.S.A. specifically asked the Times and Guardian to not publish their articles and the documents detailing the program warn explicitly and repeatedly of the need for secrecy: "Do not ask about or speculate on sources or methods." www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance
- In response to the latest revelations, Representative Rush Holt of New Jersey has introduced a bill, the Surveillance State Repeal Act, which would, among other things, bar the N.S.A. from installing such backdoors into encryption software. While a statement from the Director of National Intelligence, James Clapper—published after the reports by the Times and the Guardian—said that the fact that the N.S.A. works to crack encrypted data was "not news," Holt said, correctly, that "if in the process they degrade the security of the encryption we all use, it's a net national disservice."

3.6 NSA & GCHQ vs OPEC:

- OPEC Organization of Petroleum Exporting Countries, aim is to keep oil prices high. Not a terrorist organisation, but of interest to the US government.
- http://arstechnica.com/information-technology/2013/11/quantum-of-pwnness-how-nsa-and-gchq-hacked-opec-and-others/
- Hacking showed the Saudis had released incorrect oil production figures. The typical "customers" for such information were the CIA, the US State Department and the Department of Energy, which promptly praised the NSA for confirming what it had suspected for years. **key-9**
- OPEC was on the National Intelligence Priorities Framework**key-11** No longer; fracking has changed the political landscape.

3.7 IRAN Nuclear Power Station Centrifuges

Intelligence/hacking. Of relevance?

3.8 NSA and ISP or IXs and GCHQ: Tempora (http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa)

The NSA has its own cable-intercept programs The NSA has its own cable-intercept programs.

The division inside the NSA that deals with collection programs that focus on private companies is Special Source Operations, described by Snowden as the "crown jewels" of the NSA.

In one top document, published here for the first time, SSO spelled out the importance of these commercial relationships which come under the heading "Corporate Partner Access".

In bald terms, it sets out its mission: "Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routes throughout the world."

http://www.theguardian.com/world/interactive/2013/nov/01/nsa-tapping-cables-document

3.9 NSA vs Verizon

- National Security Agency is currently collecting the telephone records of millions of US customers of Verizon**key-13**
- The Court Order itself **key-16** from FISA Foreign Intelligence Surveillance Court (The Foreign Intelligence Surveillance Act of 1978 (Fisa) was intended to curtail the NSA's ability to use its capabilities against Americans. It was passed as part of a backlash against one of the biggest controversies of that era: the unlawful surveillance by the intelligence agencies of US political activists, trade union leaders and civil rights leaders.)
- under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk
- numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls
- Started after 9/11 by Bush... a bulk collection program of domestic telephone, internet and email records
- USA Today in 2006: Government was secretly collecting the phone call records of tens of millions of Americans, using data provided by AT&T, Verizon and BellSouth. AT&T Hacking hardware & software made at Narus**key-17**

- Influential Senator Warned in 1975: "Th[e National Security Agency's] Capability At Any Time Could Be Turned Around On The American People, And No American Would Have Any Privacy Left ...There Would Be No Place To Hide. [If A Dictator Ever Took Over, The N.S.A.] Could Enable It To Impose Total Tyranny, And There Would Be No Way To Fight Back"
- The order has been renewed.**key-21**

3.10 CIA vs AT&T

Similarly, AT&T give CIA access to their database. http://arstechnica.com/tech-policy/2013/11/cia-pays-att-to-search-international-call-database/

3.11 Lower Manhattan Security Initiative

- center is jointly staffed and operated by the NYPD along with the largest Wall Street firms**key-18**
- Pictures here: **key-19**
- 2,000 private spy cameras owned by Wall Street firms and other corporations, together with approximately 1,000 more owned by the NYPD.
- "So the computer looks essentially through all the video, finds all of the red shirts and puts it together for you."
- "Today's surveillance camera is not merely the equivalent of a pair of eyes. It has super human vision. It has the capability to zoom in and 'read' the pages of the book you have opened while waiting for a train in the subway."
- An earlier court ruling: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, e.g., People v. Weaver, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ('Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defence attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.') The Government can store such records and efficiently mine them for information years into the future."
- See "Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties."**key-20**

Bibliography

[1] http://arstechnica.com/information-technology/2013/11/googlers-say-f-you-to-nsa-company-encrypts-internal-network

[2] http://arstechnica.com/tech-policy/2013/10/new-docs-show-nsa-taps-google-yahoo-data-center-links

[3] http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

[4] http://www.spiegel.de/international/world/how-the-nsa-and-gchq-spied-on-opec-a-932777.html

[5] http://www.fas.org/irp/dni/icd/icd-204.pdf

[6] http://arstechnica.com/information-technology/2013/11/quantum-of-pwnness-how-nsa-and-gchq-hacked-opec-and-others/

[7] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[8] http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order?guni=Article:in%20body%20link

[9] http://www.wired.com/science/discoveries/news/2006/05/70908

[10] http://www.counterpunch.org/2012/02/06/wall-streets-secret-spy-center-run-for-the-1-by-nypd

[11] http://www.eastnews.pl/pictures/subject/id/00935088/section/news/page/1/

[12] http://www.constitutionproject.org/pdf/54.pdf

[13] http://arstechnica.com/tech-policy/2013/07/snowden-be-damned-government-renews-us-call-record-order/

[14] http://arstechnica.com/tech-policy/2013/06/new-leak-feds-can-access-anything-in-your-google-facebook-and-more/, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data/print, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

[15] http://www.theguardian.com/world/interactive/2013/nov/01/nsa-tapping-cables-document

Terminology

- "**third-party doctrine**." This notion says that when a person has voluntarily disclosed information to a third party—in this case, the telco—the customer no longer has a reasonable expectation of privacy over the numbers dialed or call duration. Therefore, this doctrine argues, such metadata can be accessed by law enforcement with essentially no problem.

Chapter 4

Military Intelligence 5: The UK Domestic Intelligence Agency

4.1 Origins

The UK's Security Service, also known as MI5, is the UK's domestic intelligence agency and was established in 1909, as a reaction to fears of German spying activities. Since 1936 it has also become part of the "Joint Intelligence Committee (JIC)" (Gill 2003: 268) along with the other intelligence agencies UK Government Headquarters (GCHQ), the overseas intelligence services MI6 and the other special branches. In 1957 JIC then became part of the Cabinet Office, showing a further integration into the government. Later it was heavily involved in the conflict in Northern Ireland, taking a leading role in the operations pouring almost half its resources into these operations. Furthermore MI5 employees are usually "attached to specific police or army operations as and when their specific expertise is appropriate" (Gill 2003: 272).

4.2 Official Purpose and Operations

The official purpose of MI5 is:

> "Protecting the UK against threats to national security from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthroworundermineparliamentarydemocracy by political, industrial or violent means."
>
> — *(MI5)*

The current Director General is Andrew Parker and it is based in London, with eight regional UK offices and one in Northern Ireland. It is divided in to nine branches dealing with issues such as "terrorism, espionage and the proliferationofweaponsofmassdestruction"(MI5). MI5 also provide security advice to other public and private sector security organizations.

4.2.1 Operations

MI5 mainly operate within the UK but cooperate closely with organizations such as the UK Government Communications Headquarters (GCHQ) for intelligence information and the UK's overseas Intelligence Services (MI6). Perceived threats are fought against in the following ways:

Investigation into "the suspect individuals and organisations to obtain, collate, analyse and assess secret intelligence relating to the threats"(MI5), which requires the collection of intelligence and the management of this information.

Acting against the sources of threats by compiling evidence against them and bringing them to justice

Advising "the Government and others to keep them informed of the threats and advises on the appropriate response" (MI5) e.g. protective security measures

Assisting other agencies, govt. departments in combating threats, forming partnerships is UK and non-UK agencies and contributing to "the UK's national intelligence machinery" (MI5)

Distribution of MI5 funds, suggesting its major pre-occupations:

4.2.2 Collection of secret intelligence

The collection of intelligence is deemed vital in combating threats and needs to be kept secret so that terrorists and other threats do not find out about this information. Collection is done in several ways: Firstly, through "covert human intelligence sources" (MI5) which means agents, or individuals, that are able to provide "secret reporting on a target of investigation" (MI5). Secondly it can be done through direct surveillance, or through the interception of communications. Finally, "intrusive surveillance" (MI5) can be used, such as "eavesdropping in someone's home or car" (MI5). The "Regulation of Investigatory Powers Act 2000" (MI5) limits these acts and thus they need to abide by the codes of practice this suggests. Where the law requires it "authorisation for intrusive measures obtained externally (from the appropriate Secretary of State)"(MI5) is needed, in all other cases the decision is made internally.

62% of files in stock relate to individuals (national and international), who have been under investigation at some point since 1909, just over 10% are open for investigation (MI5). The remaining are closed and scheduled for destruction or converted to microfilm. Access to these microfilmed files is only allowed with special permission.

4.2.3 Cooperation with the Special Branches

The special branches (dealing with national security) stem from the "1883 Irish Nationalist bombs in London" (Gill 2003: 268), which resulted in the creation of the Metropolitan Police Special Branch, and from 1961 onwards provincial forces also began establishing these. Only

recently have the special branches been truly integrated into the criminal investigation departments, due to the fact that previously their main duties were directed by MI5. In fact, the Special Branch officers "have been seen as foot-soldiers" (Gill 2003: 269) of MI5. Today, their function is the "investigation and surveillance of individuals and groups suspected of a variety of offences…or by way of threat assessments in advance of political meetings and demonstrations" (Gill 2003:269). This is justified part as necessary for police investigations and in part for the intelligence agencies' investigations. In 1994 there was a revision to the guidelines for the special branches, adding to responsibilities 'counter-proliferation', in terms of dealing with weapons of mass destruction and "gathering intelligence on animal rights extremist activity" (Gill 2003: 269).

4.3 Alternative Assessments

4.3.1 Recent Intelligence Scandals

British Intelligence, of which MI5 is a major part, has been closely involved in the recent US Surveillance Scandal, where whistleblower Edward Snowden leaked NSA intelligence files. British and American Intelligence Agencies have been closely linked since their respective establishments, exchanging intelligence information and facing common enemies. In the Snowden leaks, 58,000 GCHQ pages were found. This was especially 'Big Data' (the "electronic trawls across all media"(Judd 2013)) that individuals leave behind, creating much shock amongst the population. The intelligence-gathering techniques have been heavily criticized and it has been perceived by many as a salient threat to privacy and a violation of individual freedom.

However in a speech by MI5 General Director Parker, he "insisted MI5 did not have or want an all-pervasive, oppressive security apparatus" (Hopkins 2013).Indeed, to him GCHQ intelligence collection is necessary in fighting terrorism and other threats.

4.3.2 Whistleblower Annie Machon: No real oversight of operations

Annie Machon is a former MI5 intelligence officer "who resigned in 1996 to blow the whistle on the spies' incompetence and crimes" (Machon 2013). Amongst other criticisms she writes that "the application for warrants is a tick-box exercise where basic legal requirements can be bypassed, the authorising minister only ever sees a summary of a summary… never declines a request in case something literally blows up further down the line" (Machon 2013).This suggests that despite the official strict requirements for acquiring a warrant for intrusive surveillance, in practice there is not much restriction at all. Indeed even those independent commissioners who oversee MI5 only inspect it once a year, where they only see the best sides of the organizations and are prohibited from meeting any officials who are not content with the operations. Indeed, the Intelligence and Security Committee, who oversee intelligence gathering, are lied to constantly.

Her concerns are that anyone can be perceived as a potential threat to security, thus even the "occupygroupencampedintheCityofLondonorenvironmentalactivistswavingplacards" (Machon 2013).

This is extremely dangerous as in her view:

> "The central societal function of privacy is to create the space for citizens to resist the violation of their rights by governments and corporations. Privacy is the last line of defence historically against the most potentially dangerous organisation that exists: the nation state"
>
> — *(Machon 2013).*

4.3.3 Involvement with foreign representatives

It seems that the spying on foreign diplomats by Intelligence Agencies such as MI5 is in fact entirely legal under British Intelligence Laws, such as the Regulation of Investigatory Powers Act (RIPA), due to their breadth and often, unclear wording. The director of MI5 is one of the ten officials that can apply for a warrant to the home or foreign secretary on grounds such as the pursuit of national security and of economic well-being. This seems to have been used to for example "justify spying on Turkish and South African diplomats" (The Guardian 2013). The spying was, according to some critics, done with the help of the NSA.

4.4 Equivalents in other countries

USA

- Federal Bureau of Investigation (FBI)
- Director is James B. Comey (Federal Bureau of Investigation n.d.)

Russia

- Federal Security Service of the Russian Federation (FSB)
- Main successor of KGB
- Director is General Alexander Bortnikov (Government of Russia n.d.)

Germany

- Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV)
- Director is Hans-Georg Maassen (Federal Office for the Protection of the Constitution n.d.)
- At the Federal Level: Landesämter für Verfassungschutz (LfV)

France

- Central Directorate of Domestic Intelligence (DCRI) (Central Directorate of Domestic Intelligence n.d.)
- Director is Patrick Calvar (Le Point 2013)

Chapter 5

Who are the GCHQ equivalents in other countries? What is their purpose?

The main area of responsibility for GCHQ is in signals intelligence (SIGINT). The organization has a separate but complementary role to the Security Service and Secret Intelligence Service. When examining agencies in other countries which have similar responsibilities to GCHQ, it becomes clear that these agencies are usually not entirely equivalent. One aspect in which agencies differ is in their organisational structure, particularly the extent to which they are integrated into a nation's ministry of defence. SIGINT agencies in some countries also appear to have a wider range of responsibilities and operational potential than, for example, GCHQ. For example, the Russian SIGINT agencies seem to have a greater role in gathering data from media sources and enforcing Russian laws regarding media licensing. The purposes of these agencies can thus be said to differ between countries. In addition, it seems that there are some differences in the cultures of SIGINT agencies around the world. These are harder to define, however the material on the websites of different agencies gives an indication of 'cultural' differences. Indeed, the fact that some nations' SIGINT agencies do not have publicly accessible websites highlights these differences. In this section an outline of the roles of SIGINT agencies in the context of different regions of the globe and different intelligence relationships will be presented. A brief examination of the role of SIGINT in supranational organisations will then conclude this section.

5.1 The United Kingdom-United States of America Security Agreement

The intelligence-sharing community which includes the UK, USA, Canada, Australia and New Zealand and which is often referred to as the 'Five Eyes' emerged from British-American intelligence-sharing activity during the Second World War and the early years of the Cold War. The SIGINT network ECHELON is operated on behalf of these five countries, which are signatories of the UKUSA Security Agreement. One source suggests that each of these five nations has a responsibility to monitor different parts of the globe; however, it should be added that this information is not publicly known (pg. 6; December, 2012).

5.1.1 The USA

The NSA is an example of a SIGINT agency that is highly integrated into the Department of Defense. As well as managing American SIGINT, the NSA is responsible for protecting the US government's communication and information systems. The sheer size of the American intelligence community marks it out from its equivalents in other countries. GCHQ has the largest annual budget of the European SIGINT agencies at an estimated 1 billion euro, while the NSA's annual budget is reported to be $10 billion (pg. 21; General, Internal, Liberties, & Affairs, n.d.). The NSA has been one of the most heavily criticised SIGINT agencies following the Snowden leaks in 2013. These revealed multiple occasions of the NSA acting in ways which many perceive to be overly intrusive; for example, the Snowden leaks confirmed in May that a warrantless wiretapping scheme operated by the NSA had been approved by the Bush administration in 2005. The NSA's website is accessible to the public, demonstrating that the NSA recognises the need for some kind of transparency. Nevertheless, the NSA is unapologetic in stating that it helps "the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances"(NSA, n.d.-a).

5.2 European agencies

A report on large-scale surveillance activities of five European nations (the UK, France, Germany, Sweden, and the Netherlands) found that the operational capacities of the French, German and Swedish agencies with regards to budget and human resources were significantly lower than those of GCHQ and the NSA. No concrete evidence for Dutch participation in large-scale surveillance was found. There is little evidence to suggest that that EU member states' intelligence services (other than GCHQ and the German BND) are collecting data from the servers of private companies as the NSA's PRISM programme has done (pg. 20-1; General et al., n.d.). Nevertheless, it is difficult to come to concrete conclusions on this issue.

5.2.1 Germany

The TA Directorate of the Bundesnachrichtendienst (BND) is the main German agency responsible for SIGINT. The BND works together with the domestic intelligence agency known as the Federal Office for the Protection of the Constitution, or BfV (which has organisations at the state or Land level) and with the Military Counterintelligence Service, or MAD (which is responsible for the detection of counterintelligence in the German army). The BND is directly subordinate to the Chancellor's office and is thus similar to GCHQ (and different to the NSA) in that it is not integrated into the Federal Ministry of Defence1. Another link between German and British SIGINT is their common international focus: the GCHQ is under the responsibility of the Minister for Foreign and Commonwealth Affairs, and the bulk of SIGINT analysis in Germany takes place within the BND which is the foreign intelligence agency of Germany. Like GCHQ, the BND has a website which indicates an awareness of the public demand for greater transparency: "The signals intelligence collection is following complex procedures and is subject to constant legal control"(BND, n.d.-a).

5.3 Israel

Israel's SIGINT agency is generally known as Unit 8200, although it is sometimes also referred to as the Israeli SIGINT Unit (ISNU) or the Central Collection Unit of the Intelligence Corps. Unlike the GCHQ, unit 8200 is fully integrated into the Israeli Defence Forces (IDF) and is currently the largest unit in the IDF (Matthew Kalman, n.d.). Within Unit 8200, another unit known as Unit Hatzav is responsible for monitoring military intelligence-related information from media sources. The known existence of this unit seems more overt than any media-monitoring activities of GCHQ. Another notable feature of Israeli SIGINT is its links with the USA, as demonstrated by the documents leaked by Edward Snowden which revealed an intelligence-sharing agreement between the NSA and the ISNU in 2009 (NSA and ISNU, n.d.). Access to information regarding the ISNU and Aman (the Military Intelligence Directorate of which the ISNU is a part) is much more restricted than it is for the GCHQ, with Aman's website only existing in Hebrew. Furthermore, the identity of the leading Brigadier-General for Unit 8200 is classified. This contrasts sharply with the recent move by GCHQ towards at least a perception of greater transparency, as demonstrated by the Sir Iain Lobban's appearance before the Intelligence and Security Committee in November 2013.

5.4 China and Russia

When considering the role of SIGINT agencies and monitoring in the UK public sphere, it is useful to consider the capabilities and operations of countries which are popularly viewed in the West as enforcing tough restrictions on civil liberties.

5.4.1 China

The Chinese SIGINT and cryptology capabilities appear to be concentrated in the Third Department (and its affiliated Technical Reconnaissance Bureaus) of the General Staff Department, which is part of the People's Liberation Army (PLA). The Ministry of State Security also has some SIGINT capabilities, although these appear to be mostly domestic. The Third Department has counterpart agencies within the PLA's seven Military Regions, as well as in the Air Force, Navy and Second Artillery. Together, these agencies monitor communications traffic within China and may be monitoring communications from facilities abroad as well (pg. 2; Stokes, Lin, & Hsiao, 2011). Just as one responsibility of the NSA is to prevent "foreign adversaries from gaining access to sensitive or classified national security information" (NSA, n.d.-b), the Third Department is responsible for the security of the computer systems of the PLA. The greater integration of Chinese SIGINT capabilities into the military is a difference between the Third Department and GCHQ. Furthermore, given that China is a one-party state, the nature of SIGINT collection and analysis is likely to be much more politicised than it is in the UK. In addition, the MSS appears, like the domestic police, to have the power to arrest people for crimes involving state security:

> "Article 4 of the Criminal Procedure of the People's Republic of China — State security organs shall, in accordance with law, handle cases of crimes that endanger

> State security, performing the same functions and powers as the public security organs"
>
> — *(The Supreme People's Court of the People's Republic of China, n.d.)*

By contrast, GCHQ acting on its own does not have the power to arrest people. Once again, the lack of public accessibility in the form of an official website indicates the relative lack of transparency of any of China's SIGINT agencies.

5.4.2 Russia

Until 2003, FAPSI was the Russian equivalent of GCHQ and the NSA. Since then, its functions have been split between the Federal Security Service (FSB) and the Federal Guard Service (FSO), both Russian security agencies. These two agencies gather and analyse data internationally, with a main focus on the states of the former Soviet Union (Shuster, n.d.). It appears that the FSO has been assigned the responsibility of "running secure communications for state structures, and protecting them from foreign intelligence services" (Carr, 2011). Just like the NSA and the Communications-Electronics Security Group (CESG) branch of GCHQ, the two Russian agencies are entrusted with ensuring the security of government communications. A difference between GCHQ and the Russian system is the apparent binary structure of SIGINT analysis between two different agencies in Russia.

The role of Roskamnadzor should also be considered:

> "ROSKOMNADZOR is a federal executive authority entitled to carry out permitting and licensing activities, validation and supervision in the spheres of telecommunications, information technologies and mass communications"
>
> — *(ROSKOMNADZOR, n.d.)*

Roskamnadzor is responsible for the issuing of licenses to various media and communications services, and ensuring that these services comply with the prohibition on media incitement of terrorist activity set out in a regulation known as Article 4. According to one source, there is evidence that media questioning of government statements on incidents of terrorism is counted as a violation of Article 4, resulting in the revocation of media licences. In 2006 and 2007, Article 4 was amended to include "information in computer files and programs"(Carr, 2011) as well as traditional print and broadcast media. This sort of overt punishment of dissent by an executive body marks Russia's approach to intelligence gathering as different to the British approach. The fact that Roskamnadzor has a website in Russian and English suggests a degree of openness, however this is diminished by the lack of a public online presence of the FSB and the FSO.

5.5 Supranational organisations

5.5.1 NATO

At the time of publication of a 2005 NATO document, "the development of a consistent set of SIGINT-related mission tactics, techniques, and procedures for NATO assets" (pg. 11; Unclassified, 2005) was still underway. According to this publication, up to that point if NATO members decided to share information they did so in an impromptu manner; different nations had their own systems and structures for gathering SIGINT. It is difficult to ascertain intra-NATO SIGINT capabilities at present, however if changes have been made since 2005 it seems likely that they have involved aligning the security goals and SIGINT procedures of NATO members in some way. Nevertheless, given the recent revelations about the surveillance of fellow NATO members such as Germany by the USA, it seems unlikely that the sharing of SIGINT forms of ISR (Intelligence, Surveillance and Reconnaissance) has become particularly centralised.

5.5.2 The United Nations

The UN has often been reluctant to emphasise its intelligence-gathering role, and traditionally any intelligence gathering undertaken by the UN has been in the form of human intelligence (HUMINT) from direct observation by peacekeepers on the ground. Like NATO, the UN has recently been expanding its SIGINT as well as its Imagery Intelligence (IMINT) capabilities (pg. 276; Dorn, n.d.).

5.6 Footnotes

1: (BfV, n.d.)

("Spiegel Magazine article," n.d.)

(BND, n.d.-b)

5.7 Bibliography

BfV. (n.d.). Verfassungsschutz — how does the BfV operate? Retrieved from http://www.verfassungsschutz.de/en/fields-of-work/counter-espionage-and-counter-proliferation/how-does-the-bfv-operate

BND. (n.d.-a). BND website. Retrieved from http://www.bnd.bund.de/EN/About_us/Operational_Structure/TA/ta_node.h

BND. (n.d.-b). BND website. Retrieved from http://www.bnd.bund.de/EN/About_us/Operational_Structure/TA/ta_node.h

Carr, J. (2011). Inside Cyber Warfare: Mapping the Cyber Underworld, 235–239. Retrieved from http://books.google.co.uk/books?id=5LIyXzpKhYsC&pg=PA235&lpg=PA235&dq=fso+and+fsb&source=bl&ots=0T7 and fsb&f=false

December, J. C. (2012). Canada and the Five Eyes Intelligence Community, (December).

Dorn, A. W. (n.d.). UNITED NATIONS PEACEKEEPING INTELLIGENCE.

General, D., Internal, F. O. R., Liberties, C., & Affairs, H. (n.d.). National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law.

Matthew Kalman. (n.d.). The Guardian: Israeli military intelligence unit tech boom. Retrieved from http://www.theguardian.com/world/2013/aug/12/israel-military-intelligence-unit-tech-boom

NSA. (n.d.-a). NSA Mission Statement. Retrieved from http://www.nsa.gov/about/mission/index.shtml

NSA. (n.d.-b). NSA homepage. Retrieved from http://www.nsa.gov/about/index.shtml

NSA and ISNU. (n.d.). The Guardian: NSA and Israeli intelligence — memorandum of understanding. Retrieved from http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document

ROSKOMNADZOR. (n.d.). Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communication (ROSKOMNADZOR) website. Retrieved from http://rkn.gov.ru/eng/

Shuster, S. (n.d.). Time World: Snowden in Moscow: What Russian authorities might be doing with the NSA whistleblower. Retrieved from http://world.time.com/2013/07/10/snowden-in-moscow-what-are-russian-authorities-doing-with-the-nsa-whistleblower/

Spiegel Magazine article. (n.d.). Retrieved from http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html

Stokes, M. A., Lin, J., & Hsiao, L. C. R. (2011). The Chinese People ' s Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure.

The Supreme People's Court of the People's Republic of China. (n.d.). The Supreme People's Court of the People's Republic of China: Criminal Procedure. Retrieved from http://en.chinacourt.org/public/detail.php?id

Unclassified, N. (2005). NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) VOLUME 1: Architecture Description (Vol. 1).

PART II

THE FUTURE

Chapter 6

Do all laws need to be public and how can one legislate publicly while maintaining secrecy, or legislate secretly while maintaining public confidence?

A key component of law is its universality. Applicable to all equally, is the mantra at the heart of our legal system that results in us reaching to it as an arbitrator. On this alone there is no contradiction in having regulations which go unseen – possibly even by those beholden to them. Such an image is, however, less than satisfying. If a rule affects us directly, we feel slighted if we are condemned, be it as simple as 'don't walk on the grass', if there was insufficient information on it, such that we were ignorant of our wrongdoing when we committed it. Lying behind this is a sense that justice can only be meted out on those who understand that their actions are wrong. A case in point would be or attitudes towards mental health in the criminal justice system, or the legal age of responsibility. Does this continue though into those regualtions that affect me only indirectly – for example, those which might cover building regulation or required minimum size of the 'small print' on a contract?

Here experience suggests that we do again feel that even though we might not discover the details of the law, unless we suspect we have been mistreated, the information needs to be publicly available. Such that I can check, if I so wished that the contract I was signing or having signed was valid, that there is a legal argument to be had about the height of my neighbour's new shed. The examples might seem trivial but the nature of our response to injustice transfers directly.

Awareness is crucial if we are to feel that justice has been done. Furthermore, for a democratic society the key check on all public offices, and on whether law is being implemented correctly is that it is open at all times to public scrutiny. In this sense legal secrecy is anathema to the democratic process which relies on the watchers having no one to watch but other watchers. In addition to being unable to be sure a law is being enforced without openness, is there not

a risk of a worrying trend hinted at previously? That if there is a precedent for parliament creating laws in secret in relation to one thing, how can a democratic society be sure the same does not happen elsewhere? In addition, precedent is itself a major part of British common law. Custom does dictate action, but would jurors or judges necessarily be allowed access to related case history if by dint of allowing for secret laws we are acknowledging that there is some information which should have a highly restricted audience, an audience that might not always include our jurors or judges?

Essentially the problem we are faced with is that secret laws in the sense that we as a society conceive of them are incompatible with secrecy. To be just and consistent public knowledge is essential. This is not necessarily to dismiss specific regulation for the intelligence agencies, but it will be internal to them and cannot be binding in the way a normal business or gov-ernment department would be. Intelligence agencies perhaps should be beholden to laws they break, but in that age old adage you are only guilty if you are caught. The intelligence agencies operate extra-legally, and this will be as true if the regulation in place for them is secret, as if they are unregulated. Maintaining the public's trust even when all is open can be challenge enough. Introducing a secret element compounds this problem. In addition the need to with-hold information if legislating publicly undermines the effort of doing so. In effect you are legislating in secret as much of the key information is kept back. It would seem therefore that all law must be public and that as a result we need to accept that intelligence agencies, as long as they demand secrecy, will always operate in an extra-legal environmentThe law cannot effectively engage with them without compromising either itself, the secrecy of the organisation or public confidence. To be effective in the way they claim, intelligence agencies must operate in the same environment as those they seek to thwart, be it criminal gang or terrorist cell, and in so doing they must be operating outside the law. Ultimately this makes codified structures ineffective in regulating them. When those performing acts they feel to be either disproportionate or unethical there needs to be a clear method of raising this and recourse to appeal to the ISC regardless of the directions of senior figures at GCHQ

6.1 Proposals

The intelligence services need to be subjected to quarterly review by the ISC, and the conclu-sions published publicly. Ideally said publication ought to be enacted through major national newspapers, the BBC and the UK government website, to ensure that it will be encountered by those browsing as well as those explicitly searching for it. In addition each report should be submitted to parliament for approval before being deemed complete. The ethics committee, proposed under 'How to blow the whistle in an intelligence agency', must become a key com-ponent of diseminating concern. We are reliant on a culture of honesty to effectively regulate the intelligence agencies and should not resort to a second 'dark' legal system with exemptions and exceptions not found currently. The legislation needs to be kept public and as a result it must fall to the ISC to condemn practices deemed unethical or excessive, and if necessary ap-proach the police to launch a formal investigation into the actions of the intelligence agencies in question. We may accept extra-legal activity to a point, one which ought to be defined by the ISC or the elsewhere proposed Ethics committee. Those disproportionate actions themselves

should become known through an effective complaints procedure (see How to blow the whistle in an intelligence agancy) Where this has been seen to have taken place those responsible need to face public justice to maintain public and parliamentary trust in the operations of our intelligence agencies. When those performing acts they feel to be either disproportionate or unethical there needs to be a clear method of raising this and recourse to appeal to the ISC regardless of the directions of senior figures at GCHQ or elsewhere.

Essentially legislation must not become secretive and should not act as the prime means of regulating the intelligence community.

Chapter 7

Britain and its role in the NSA scandals

In 1929, US Secretary of State Stimson decided to close down the Black Chamber, the forerunner of the National Security Agency (NSA). Upon hearing of the secret activities of the organisation, he replied that "gentlemen do not read each other's mail" and, seeing no value in the clandestine operations, withdrew its funding (Richelson, 1995).

Almost a century later, the United States and the United Kingdom do not only read, but also generously share the 'mail' that they are able to intercept. From papers leaked by NSA whistleblower Edward Snowden in the summer of 2013, it has become clear that the United States has been tapping not only its adversaries, but also its allies, including Germany and France. As details started to surface about the attempt of the NSA to even monitor friendly heads of state, the intelligence agencies of the United Kingdom also came under increasing pressure to release details about its methods (Spiegel Staff, 2013). In recent months, it has become clear that GCHQ and the NSA have been collecting enormous amounts of information, using only a small percentage of it and officially discarding the vast majority (MacAskill, Borger, Hopkins, Davies, & Ball, 2013). With this undertaking, called Operation Tempura, GCHQ "reportedly sucks up 21 petabytes [1 million gigabytes] of data each day, stores it in a central database, sifts it, and shares it with its US equivalent, the NSA" (Nielsen & Rettman, 2013). The operation, that has been running for almost two years, allows GCHQ to tap into and store these huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. GCHQ and the NSA are consequently able to access and process vast quantities of communications between "entirely innocent people, as well as targeted suspects" (MacAskill et al., 2013).

These revelations focused not only on the methods used by the intelligence agencies, but also on the legality of such operations. Many reports indicate that the NSA and GCHQ have been looking for and utilising lacunas in their respective legal systems in order to legitimise their operations, which calls into question whether the legal frameworks of both nations are adequate.

This section will address the issue of intelligence sharing with other nations, particularly with the United States. It will focus on the existing legal framework and how both states have been trying to work their way around them, using the Snowden papers as its basis. Moreover, it will give recommendations on possible policies and improvements in the legal systems that could be implemented by the two states in order to minimise the possibility of unrestricted, uncontrolled intelligence gathering.

7.1 The history of Anglo-American cooperation

Before the Second World War, the United Kingdom was far ahead of the United States in its capabilities in the field of signal intelligence (SIGINT) and communications intelligence (COMINT). Bletchley Park, the headquarters of the forerunner of GCHQ, was able to collect incredibly important intelligence on the Axis powers and often shared it with its wartime allies. After the war, the cooperation was made official in the United Kingdom — United Stats of America (UKUSA) Agreement, which, after it was joined in subsequent years by Australia, New Zealand and Canada, was referred to as the 'Five Eyes Agreement'. Other friendly nations, such as West Germany, joined the community and became known as 'third parties' (Norton-Taylor, 2010).

Over the decades that followed, GHCQ and the NSA have come to work together so closely that "since the 1970s, with processes and projects, at various points GCHQ and NSA are effectively the same organisation" according to Richard Aldrich, the well-renowned historian and author of the unofficial history of GCHQ (Quinn, 2013). It is exactly this alleged symbiosis between the two organisations that has led to extensive criticism in Parliament and in the media, saying that GCHQ was not operating in the framework of British law anymore. But what does the British legal framework look like exactly, and how would it be possible for GCHQ to successfully circumvent it?

7.2 The British legal framework for intelligence gathering and sharing

In hearings in Parliament in the summer of 2013, Foreign Secretary Hague defended the British legal framework concerning the gathering and sharing of intelligence, stating that "the law is actually quite clear. If the British intelligence agencies are seeking to know the content of emails about people living in the UK then they actually have to get lawful authority. Normally that means ministerial authority. That applies equally whether they are going to do the intercept themselves or whether they are going to ask somebody else to do it on their behalf" [Emphasis mine] (Watt, 2013). Hague told the MPs that the received "hundreds of requests a year" from both GCHQ and MI6 to approve operations, as is required by the Intelligence Services Act of 1994 (hereafter: 1994 Act) and the Regulation of Investigatory Powers Act of 2000 (hereafter: 2000 Act) (Watt, 2013).

A report on the topic of Rendition, issued in 2007 by the Intelligence and Security Committee, came to a similar conclusion with regard to the rendition policies of the government. It noted that "Security Service and SIS use a system of safeguards to ensure that their intelligence does not result in torture or mistreatment. These safeguards take the form of conditions which restrict the use that a liaison partner may make of UK intelligence" (Security and Intelligence Committee, 2007).

All three major intelligence agencies of the United Kingdom are thus required to seek ministerial approval for their actions and are officially bound in various legal frameworks, which were designed to limit the possibilities of unlawful intelligence gathering and sharing. However, as Secretary Hague already noted, this "lawful authority" normally implies ministerial authority.

As will be explained later, he probably referred to a lacuna in the 2000 law, one that was allegedly used by all three agencies to an extent that made it practically possible to circumvent the law's most substantial provisions and intentions.

7.2.1 The alleged circumvention of the law

Of all three agencies, the allegations vis-à-vis GCHQ of circumventing the British legal system are the most salient. As Foreign Secretary Hague correctly mentioned, the 2000 Act does indeed require that the tapping of defined targets is authorised by the Home Secretary or Foreign Secretary. However, as the Guardian noted, the Act also contains an "obscure clause" [2000 Act, Chapter I, Section 7] that would allow the Foreign Secretary to "sign a certificate for the interception of broad categories of material, as long as one end of the monitored communications is abroad. But the nature of modern fibre-optic communications means that a proportion of internal UK traffic is relayed abroad and then returns through the cables" (MacAskill et al., 2013). This loophole had not been intended when the Act was drafted and was also probably not foreseen due to the different nature of communication intelligence back then. However, in the setting of 2013, the clause enables the Foreign Secretary to give the agencies a de facto carte blanche in certain areas of intelligence gathering.

For any intelligence that might not be retrieved via this way, the British intelligence services seem to have chosen for another option: to let the Americans gather and subsequently share the information. The relationship between British and American intelligence services is a close one not only in the metaphorical sense but also in a physical one. Since 1954, the Americans have had a base in the north of England called 'Menwith Hill Station'. Whilst it is officially an enterprise of the Royal Air Force (RAF), Annie Rainbow of the Campaign for Accountability of US Bases noted that "even those with the most limited knowledge of what goes on at Menwith Hill know it is not an RAF base. It is run by the NSA and they are totally unaccountable to British law", and the Americans regard the base to be under their jurisdiction despite it being on British soil (Blackhurst & Gilbert, 1996). The NSA has been accused of using the base to obtain intelligence on British subjects in Britain that their British counterparts are not allowed to access without a warrant of the Home or Foreign Secretary. Allegedly, this intelligence was subsequently shared with not only GCHQ, MI6 and MI5, but in some cases also with American companies, which were then able to use the information to "steal a march on European firms to win a huge Saudi Arabian commercial airliner order" (Blackhurst & Gilbert, 1996). Thus, the NSA would hereby be not only assisting British agencies in work that they are not permitted to carry out themselves, but also be conducting economic espionage against a friendly nation.

This practice of the NSA offering information to its British counterparts was also confirmed in a Parliamentary hearing by David Blunkett, the former Home Secretary at the time of the 9/11 attacks. He told MPs: "Yes we do need to dampen down fear, yes we do need to reinforce the fact that we are engaged in international cyberattack and the dangers that come from international global terrorism. But in doing that, in reinforcing and reassuring people about the way we handle their data, can we take a closer look at how other agencies — including the NSA and our friends and colleagues in the US — use material gathered from network and service providers and offer it rather than having it sought from them in a way that makes authorisation extremely difficult?" (Watt, 2013). Moreover, he noted that "the system would

appear to allow GCHQ to bypass formal legal processes to access personal material, such as emails and photographs, from the world's biggest internet companies" (Watt, 2013).

Other sources, too, comment on the involvement of private companies in the practices of the NSA and British intelligence services. The papers that were obtained by Edward Snowden (and which he passed on to the Guardian) suggested that companies were paid for co-operating, under secret agreements, with intelligence services, and "GCHQ went to great lengths to keep their names secret. [...] Staff were urged [...] to disguise the origin of 'special source' material in their reports for fear that the role of the companies as intercept partners would cause 'high-level political fallout'" (MacAskill et al., 2013). According to Reuters, the companies "were forbidden from revealing warrants that compelled them to allow GCHQ access", a statement that was confirmed by Guardian sources (O'Brien, Holden, & Hosenball, 2013).

The Guardian moreover reported that whilst the Americans were given guidelines for the use of the intelligence they would gather, they were told in legal briefings by GCHQ lawyers: "We have a light oversight regime compared with the US". They were also told that with regard to judging the necessity and proportionality of the intelligence they would be looking for, it was "your call" (Watt, 2013).

As was noted before, the amount of data that are obtained in this way is enormous, and the titles of two main components of GCHQ's programmes: Mastering the Internet and Global Telecoms Exploitation, which aim to collect as much online and telephone traffic as possible. As the Guardian noted, this was "all being carried out without any form of public acknowledgement or debate" (MacAskill et al., 2013).

7.2.2 Britain's official rationale

It has become clear that the British intelligence agencies have collaborated with their American partners by using an Act of Parliament in a way in which it was never intended, and by using American sources to obtain information in ways for which it would be very hard for British services to be given the authority for. If British intelligence agencies were confident that the results of these acts were of such great importance to national security, why did they never seek to adjust the legal framework instead of using the lacunas of the old one? Why would they let the danger of publicity about such questionable methods hang above their heads as a sword of Damocles instead of initiating reforms?

One of the explanations that has been brought forward is one that is intimately linked with one of the greatest challenges that security and intelligence services face: the issue of secrecy of intelligence operations and fact that possible adversaries are always able to listen in on public debates.

Probably more important, however, it the relationship between British and American intelligence agencies. In 2010, when an appeals court forces the UK government to disclose intelligence related to a case in which British intelligence services had cooperated with the Americans, the agencies argued that such disclosure could jeopardise future intelligence sharing (MacDonald, 2010). Moreover, in relations to cases of terrorism and rendition, the heads of the

three main intelligence agencies have often reiterated that sharing intelligence was instrumental to the effectiveness of the agencies, and in particular the intelligence that it received from the United States was said to be very valuable. Any change to the status quo, which might be the result of a public debate or of new legislation and that would curb the possibilities of intelligence sharing among Washington and London might be regarded by the intelligence agencies as detrimental not only to their operations but also to national security.

In the wake of the fallout following this summer's revelations, both UK and US government and agency officials have often declined to comment on substantive issues. Foreign Secretary Hague merely told Parliament that GCHQ "always adhered to British law when processing data gained from eavesdropping" and that he "could not confirm or deny any details of UK-U.S. intelligence sharing, saying that to do so could help Britain's enemies" (O'Brien et al., 2013). GCHQ and NSA spokespersons echoed his arguments, and NSA spokeswoman Judith Emmel "rejected any suggestion the U.S. agency used the British to do things the NSA cannot do legally. Any allegation that NSA relies on its foreign partners to circumvent U.S. law is absolutely false" (O'Brien et al., 2013). However, the accusation that the relationship was the other way around, and that the UK asked the NSA to collect intelligence that GCHQ was not allowed to obtain under British law, was not addressed. Moreover, whilst national security is understandably a great concern of government and Parliament alike, it should not be used as a catch-all cover for many questionable types of practices, nor should it allow officials to sweep sensitive issues and possible circumventions of the law under the carpet.

7.3 Possible policies

What kind of policies could or should be implemented, then, in the coming months and years in order to prevent the problems that have been described above? How can the need for an effective intelligence apparatus be balanced with fundamental rights to privacy of British citizens, in particular in the framework of Anglo-American cooperation in this field?

First of all, government and agency officials as well as Parliamentarians and journalists should engage in a public debate about intelligence gathering and sharing. Whilst chief officials of the government and the intelligence agencies have repeatedly tried to cover their actions by upholding national security as sacrosanct, a more fundamental public debate is an absolute necessity to guarantee the legitimacy of the intelligence agencies' activities as well as the functioning of intelligence gathering at large. Both British and American intelligence services have experienced a sharp decline in public trust and confidence, and whilst it is often said that intelligence agencies should not be interfered with in order to guarantee and maximise their effectiveness, it seems clear now that this decline threatens the precarious balance between effectiveness and legitimacy that is at the basis of any intelligence apparatus in a democratic system.

Secondly, the legal framework underlying both domestic intelligence gathering as well as the procedures of intelligence sharing are in dire need of reform and renewal. This would be the case for three particular provisions or areas of law:

1. The abovementioned "obscure clause" of the 2000 Act [2000 Act, Chapter I, Clause 7] is clearly outdated. Whilst it might have been of use in the framework in which it was embedded at the time the Act was passed, it now leaves too much room for possible surveillance and intelligence gathering by the agencies without any form of parliamentary, judicial or other form of control.

2. The American base at Mendith Hill, whilst officially operating under the RAF, has allegedly been instrumental in the circumvention of British law with regard to intelligence gathering. It would be up to the government of the UK to launch an investigation into this matter, and if the allegation would hold, then it should undertake actions. As the activities of the NSA could and should be regarded as impeding upon the sovereignty of the United Kingdom, it should be made clear that bases on British soil, even when they are mostly populated by American officials, fall under British jurisdiction and should thus abide by British law. These rules have not been adequately lived up to in the past and whilst it might have been done with the (tacit) agreement of the government, it still leads to a situation of too little oversight and control by the appropriate bodies. It is up to the Parliament to hold the government and its agencies accountable for these actions and to press for further and stricter legislation if it is deemed necessary.

3. There are clear discrepancies between American and English law, or at least in the application of such law, with regard to intelligence gathering and sharing. The most effective and simple, yet also radical solution would be a complete streamlining of both American and British legal acts with regard to intelligence gathering and sharing, with similar systems of accountability and reach, as well as inter-state accountability. However, seeing as this will probably lead to resistance in both countries' domestic spheres, it might be advisable to start with the streamlining of laws with regard to intelligence sharing and intelligence gathering of citizens. This not only means more attention to living up to the current laws, as was explained in the point above, but also of implementing a new system that in itself ensures more effective control and fewer options to circumvent existing legal frameworks.

7.4 Bibliography

Blackhurst, C., & Gilbert, J. (1996). US spy base "taps UK phones for MI5." Retrieved November 25, 2013, from http://www.independent.co.uk/news/uk/home-news/us-spy-base-taps-uk-phones-for-mi5-1364399.html

MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013). GCHQ taps fibre-optic cables for secret access to world's communications. Retrieved November 25, 2013, from http://www.theguardian.com/uk/2013/ju cables-secret-world-communications-nsa

MacDonald, A. (2010). U.K. Move Could Hinder U.S. Intelligence Sharing. Retrieved November 25, 2013, from http://online.wsj.com/news/articles/SB10001424052748703455804575057550493911866

Nielsen, N., & Rettman, A. (2013). UK spy chiefs defend mass-snooping on Europeans. Retrieved November 25, 2013, from http://euobserver.com/justice/122030

Norton-Taylor, R. (2010). Not so secret: deal at the heart of UK-US intelligence. Retrieved November 25, 2013, from http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released

O'Brien, R., Holden, M., & Hosenball, M. (2013). British spy agency taps cables, shares with U.S. NSA — Guardian. Retrieved November 25, 2013, from http://uk.reuters.com/article/2013/06/21/uk-usa-security-britain-idUKBRE95K10620130621

Quinn, B. (2013). Another US-UK "special relationship" — between intelligence services. Retrieved November 25, 2013, from http://www.csmonitor.com/layout/set/r14/World/Europe/2013/0614/Another-US-UK-special-relationship-between-intelligence-services

Richelson, J. (1995). A Century of Spies. Intelligence in the Twentieth Century. Oxford: Oxford University Press.

Security and Intelligence Committee. (2007). Rendition. Retrieved from http://www.fas.org/irp/world/uk/rendition.pdf

Spiegel Staff. (2013). Embassy Espionage: The NSA's Secret Spy Hub in Berlin. Retrieved November 25, 2013, from http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

Watt, N. (2013). NSA "offers intelligence to British counterparts to skirt UK law." Retrieved November 25, 2013, from http://www.theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett

Chapter 8

Terrorists: Criminals or Enemy Combatants

Enemy combatants are afforded certain rights by the Geneva Convention**key-1** one of the core international laws that govern the behaviour of nation states in a war. There is a definite distinction between the criminal justice system and laws of war, and holding terrorists to account under one or the other system will allow for different capabilities of an intelligence agency.

Indeed, the two systems are different in their aims: the criminal justice system would aim to deter and adjudicate after an attack, whereas treating a terrorist as an enemy combatant would allow for strenuous interrogation, the aim of which is to prevent attacks before they occur.

So whom does the Geneva Convention protect? Terrorist organisations are neither nation states nor state actors (such as a state media) and are combatants who have not signed up to the Convention. In fact, terrorists often blend in with and attack civilian populations, in direct contravention of international miltary law. Under these conditions, terrorists are not protected by the Geneva Convention.

If terrorists are enemy combatants, a number of questions are immediately posed:

- How do we control our military and intelligence agencies to reflect our societal values? Treating terrorists as enemy combatants can allow for blanket detention of suspects under little evidence, as in the case of Guantanamo Bay. Here those accused of terrorist activities, are detained without charge or access to counsel, undergo a full range of interrogation techniques, have no mechanism of defence, and no way to find the reason for their detention.
- Are we safest labelling terrorists as enemy combatants? Post 9/11, how has the Western world's War on Terror affected the safety of the Western civilian and military populations?
- Where does one draw the line between a terrorist and a criminal? If a gang member kills a police officer, is he or she a combatant? If the same gang member steals a loaf of bread, she he or she a combatant?

is missing... The remainder of this section of the paper aims to discuss the above questions.

8.1 Shoot to Kill

A little about the shoot to kill policy, in Northern Ireland.

Bibliography

[1] http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/

Chapter 9

Security Ethics

Every few years, something leads society to criticize the objectives, methods or practices of British intelligence agencies.

> Intelligence is a valuable survival trait when you have to deal with the threats from the natural world. But intelligence is an even more valuable survival trait when you have to deal with the threats from other intelligent individuals. An intelligent adversary is a different animal, so to speak, than an unintelligent adversary. An intelligent attacker is adaptive. An intelligent attacker can learn about its prey. An intelligent attacker can make long-term plans. An intelligent adversary can predict your defenses and incorporate them into his plans. If you're being attacked by an intelligent human, your most useful defense is to also be an intelligent human. Our ancestors grew smarter because those around them grew smarter, and the only way to keep up was to become even smarter.
>
> — *Schneier, 2012, Chapter 2*

Schneier talks here about intelligence in the biological sense, but the quote applies to our secret finders and keepers too. Intelligence Agencies exist to anticipate and prevent threats to the government and masses of people, before they occur. This is a highly ethical principle, imperative for a state to operate and a precondition for modern liberty's individual freedom.

9.1 Threats

Fix this paragraph

Broadly, the specific threats that cause the need for intelligence agencies today, can be classified into three categories: Economic threats; Terrorist threats; Espionage & Serious Crime. Economic Intelligence is important in maintaining national competitiveness, as it is used on one hand, to assess the state's "national industries"(Luong, 2009: 164), investigating which need further development, and those abroad. On the other it also performs the function of countering economic espionage, "the acquisition of industrial technology and proprietary trade information" (Luong, 2009:165). This is critical when considering issues harmful to Britain's

economy, such as the suggestions of Chinese hacking (Rayment, 2011) or companies acting as a front in Britain.

Terrorism also continues to be a threat, in addition to espionage and serious crime, such as the Mexican drug trading networks. This is mostly what Intelligence Agencies, such as GCHQ do: "It takes an interest in places such as the Horn of Africa, Iran, and North Korea; it takes an interest in energy security, nuclear proliferation, and in state-sponsored computer hacking" (Lanchester, 2013). It is simply impossible to ignore the fact, that Britain does have enemies, and therefore needs protection.

9.1.1 Abuse from within

Systems to monitor and investigate secret organizations face a fundamental problem: the people under scrutiny are experts in hiding whatever they want. The potential for abuse is vast. One cannot use institutional pressures such as the law, or security systems such as audits, to police intelligence agencies. The only control is ethics.

9.2 What are ethics?

Whom does security secure?

That something is ethical is predicated on its moral acceptability. What is morally acceptable? Morals are largely a socially constructed ideal that shapes the institutions of that society; in Britain (a liberal democracy) these are equality between people, individual freedom (a life separate from government/politics) and fundamental rights. These differ from cnacient freedom: the collective always comes before the individual. In particular, the "right to respect for private and family life, his home and his correspondence" is incorporated into law via the European Convention of Human Rights (ECHR) (**ECHR2013**).

It is fundamentally hard to preserve these values in all circumstances, but that is where governmental institutions should strive. The principle of secrecy is undemocratic, despite historically overwhelming democratic support. The drive of Intelligence Agencies to preserve liberty by sacrificing it, compromise rights to privacy, and individual freedom itself. It is possible to do more harm than good.

The concept of finding a balance between security and liberty rests on the assummption that decreasing liberty does not decrease security. This is wrong.

> The debate isn't security vs privacy. It's liberty vs control. — *Schneier, 2008*

9.2.1 Limits to Ethics and Privacy

Security is an important component of freedom, just as freedom is an important component of security. And that is part of the problem. The battle is between our freedom as people living in society, and the freedom of intelligence agencies (and police) to operate without restriction. It may be that intrusive surveillance in Britain is the only way to achieve security for people. In this case, morally unacceptable snooping by intelligence agencies becomes ethically acceptable.

9.2.2 The value of privacy in an age of technology

Surveillance costs are miniaturizing along with surveillance equipment. Fixed costs are decreasing, data is higher quality, and tools suitable for analysis are commonplace. Estimates suggest Britain had more than 1.85 million surveillance cameras in 2011 (Lanchester, 2013). Privacy has changed as personal data becomes more valuable; new generations post images, ilocations and thoughts to the world in perpetuity. But privacy has not lost its importance. The irony is we as individuals face the same problem of security classification with which intelligence agencies struggle. Our "top secret" may be our bank authentication details or our search history.

9.3 To what extent can jurisdiction ensure ethical behavior?

9.3.1 Importance of the Law

The law can be regarded as the primary buffer between government and the masses: a protection against the infringement of modern liberty and rights. It is vital, in a liberal democratic system such as Britain, to ensure that the individual is preserved. It also provides a guide for the actions of individuals and institutions. Laws can create an uneasy balance between directly protecting individual rights and freedoms and giving intelligence agencies enough freedom to protect these through promoting security. Care needs to be taken in methods of data collection & processing; the law can normalize this concept. The "human factor" in intelligence agencies will always limit the extent to which effective laws are obeyed and one might attempt to limit this through stricter jurisdictio and one might attempt to limit this through stricter jurisdiction. When all those activities are secret, trusted oversight is paramount. Parliament, and (indirectly) the people must hold intelligence agencies to account, despite ignorance of their activities.

9.3.2 Weakness of the Laws

The Regulation of Investigatory Powers Act (RIPA) of 2000 replaced the Security Service Act of 1989, supposedly defining ethical behaviour for intelligence agencies. Yet the wording is vague; the Investigatory Powers Tribunal (IPT) state "the wording in Part II [of RIPA] presents some difficulties for the reasonable reader" . Ambiguity is a blessing for intelligence agencies.

R. Hopkins, 2013a

For example, under section 1(1)(b) it is an offence to intercept intentionally "any communication in the course of its transmission, by means of a public telecommunications system," if one does not have the lawful authority to do so . reports the court case in which Justice ruled that this did not extend to answerphone messages. Hacking with no explicit judicial right is entirely lawful. RIPA's scopr is unrestricted, leading to investigations of petty crime such as littering, or against non-criminal activists .

RIPA 2000

R. Hopkins, 2013

Who?

Schneier 2008?

US-UK Collaboration

Fix this

A GCHQ leaked internal brief PowerPoint slide also states that SRA (an unexplained acronym) "authorizes receipt of 2P intelligence on UK based targets where GCHQ has no authorization" (Lanchester, 2013). 2P is an acronym for 'second parties', meaning countries such as the USA, Canada, Australia and New Zealand. This lead to recent scandals, such as the tight collaboration between the US and UK where the US' National Security Agency's Prism program and subsequent collection of data on UK nationals, was discovered to be transferred to GCHQ. In addition, it has been suggested that a secret deal between the two countries allowed "the NSA to unmask personal data about Britons not suspected of any wrongdoing" (N. Hopkins *&* Taylor, 2013) and store large amounts of such information such as mobile phone/fax numbers, emails and IP addresses. This is especially worrying when considering the fact that even communications 'within' Britain may pass through the USA. Thus, local British laws have been avoided through the USA. Such agreements should be placed under close scrutiny to ensure that they are truly adequate and necessary to protect British citizens and that the best is done to protect their privacy.

Tempora

GCHQ's Tempora program allows it to tap undersea fiberoptic communication cables, intercepting and storing meta-data (everything but the actual content of the communication, e.g. communicating parties, duration, location). The UK connects directly to 57 countries by fiberoptic cables, and the USA to 63 .

Dance, 2013

Encryption

This section is very important, and needs rewriting then expanding greatly, especially in the context of information assurance aspects of GCHQ.

Encryption has been another issue, as the recent Snowden leaks revealed the successful cracking, of online encryption by GCHQ (and NSA). This is something that people thought protected their privacy in terms of personal data (e.g. online banking), e-mails and other online activities (Ball, Borger, Greenwald, *&* Weekly, 2013). This has been achieved by collaboration with tech-companies and Internet service providers such as Google, inserting secret 'backdoors' or weaknesses into their systems, which make access easier. A GCHQ team has in fact been working on developing ways into encrypted traffic of the major service providers: Hotmail, Yahoo, Google and Facebook (ibid.). By 2015 GCHQ had hoped to crack 300 VPN's and 15 major Internet Companies codes. This undermines the very idea of Internet security. It is clear that such measures could be critical to Intelligence Agencies in catching threats to the United Kingdom. Under such circumstances surrendering some privacy is understandable and even necessary. However, this should be done only with clear reason and be regulated by law.

9.3.3 Privacy International Statement of Grounds

The NGO *Privacy International* has petitioned the IPT to investigate direct abuse of ECHR articles 8 and 10 by the intelligence agencies. The grounds are: "soliciting and/or receipt of private information about those located in the UK from US authorities and [...] the interception of vast quantities of electronic data on fiber optic cables leaving the UK and the sharing of that data with US authorities" . Big Brother Watch and the Open Rights Group are challenging the legality of data collection methodsat the European Courts.

Privacy International, 2013

which?

9.3.4 Weakness of the Intelligence and Security Committee (ISC)

Citations, then rewrite

The Intelligence and Security Committee of Parliament (ISC) comprises Members of Parliament (MPs), many ex-ministers, such as the current chair, former Foreign Secretary Sir Malcolm Rifkind. It has been claimed that some of the members are not sufficiently detached from government and the Intelligence Agencies, to be able to provide clear judgment. On the other hand, some have argued that these ties can be beneficial as they allow for a better 'insider' view of Intelligence Agencies. It has also been criticized, that the Committee has been reacting to events only as n their role. A competent body, with no political affiliation, could establish public confidence that agencies operate ethically.

Defty, 2013

This isn't what it shows. It shows that they can't/won't disclose classified material

9.3.5 The management of collected data

Access management is a hard problem. Too restrictive and data cannot be use (actually, people will just avoid the restrictions. Feynman (2006) tells how Frederic de Hoffman, declassifying documents at Los Alamos after World War II, stored copies of everything needed to develop a nuclear bomb in his nine easily-cracked cabinets. The secure library wasn't open at weekends.) Some 80,000 officials had access to files leaked by Edward Snowden . There is no transparency; the public can never know how many people (and with what clearances) can access personal data.

N. Hopkins & Taylor, 2013

9.3.6 Limits to Law: The Role of Culture and Adaptation

The law is just one form of societal pressure. Only moral and reputation pressures can encourage trusted behaviour.

The security world changes extremely quickly and novel technologies challenge privacy in new ways. We need technologically invariant laws (Schneier, 2012).

9.4 Proposals to ensure ethical behavior

9.4.1 Regulation of Investigatory Powers Act 2000 Digital Rights section

Technology has superceded current laws. Therefore I propose an addition to the RIPA in terms of a clearly worded and precise section addressing stronger protection of privacy in the technological realm.

- **Create a boundary to bulk data collection.**
- **Ensure digital data is only intercepted under a judiciary warrant.**

Thus, only when there is sufficient cause for interception, when the privacy that is infringed upon is proportionate to the good in terms of security this could promote, when there is no hidden agenda, where the prospect of this interception being successful and useful is reasonably high, and finally that it really is the last resort in tackling a potential threat.

9.4.2 International Legal Harmonization

Harmonization of laws among the Five Eyes (or at least US-UK). Need to redo following text.

This should include clauses such as the need for warrants from the other's judiciary representatives, for the collection and retention of data from the other, like the ones needed at the local level. A committee of both British and American judges, chosen by the heads of state with long-term terms in office to ensure continuity and stability, could oversee this collaboration, being allowed access to any information deemed necessary for investigation and to ensure that the laws are respected.

9.4.3 Establishing & maintaining public trust

- **Establish a committee, trusted by**
  - **those working at intelligence agencies, to not disclose secret material, and**
  - **the general public, to not ignore ethics failures**

  to inform the public whether intelligence agencies are operating ethically.
- **Publish periodic reports of intelligence agencies' achievements**

In addition to the Interception of Communications Commissioner, his team, and the Intelligence and Security Committee, there should be an external body with minimal political affiliation who can assess the quality and necessity of intelligence methods. This could increase the likelihood that intrusive gathering is only used when

- the threat is immediate,
- the measures are likely to succeed, and
- they are the only means possible to protect the British people.

This would mean allowing a group of non-politicians to check that what is hidden is truly necessary and lawful. This group should comprise experienced judges and Human Rights leaders (public figures), selected by parliament, who keep their positions for several years .

This sounds like an optimistic view of the House of Lords...

It is crucial that as a general rule, these individuals have minimal ties to the Intelligence Agencies and no political or economic interest in their activities or security industries. The hard problem is finding people (individuals or categories) whom both intelligence agencies and the public can trust.

Periodic (perhaps every 5–10 years) reports of the achievements of intelligence agencies will help put their secrecy into context. These reports would contain no classified material.

9.5 An Ethical Culture

A culture of respect for the public, the law, and ethics is crucial inside intelligence agencies. The culture in an organization is established by management, training, and recruitment. New employees should respect the ethics of their industry (one advantage intelligence agencies have over terrorist organisations — see Shapiro (2013)), training should emphasize the importance of ethics, and managers must reward ethical behaviour (punishing actions that are unethical). It is important that employees can easily voice their concerns about potential abuses, by other members or superiors, through anonymous or pseudonymous systems. Agencies must protect such individuals.

Clarify the next paragraph, link to whistleblowing section

Due to the large amount of secrecy, the Intelligence Agencies seem to lack a culture of self-regulating caution i.e. the assumption that what they do, could come out eventually and must therefore be truly useful and completely justifiable. For example, in 2009 all GCHQ communicated, was that the encryption scheme needed to stay extremely secret, as it could have terrible consequences if leaked, such as “damage to industry relationships” (Ball et al., 2013) and unwelcome publicity This did not seem to include the idea that such a leak was quite possible or reflection upon the legitimacy of such actions. Implementing the idea that this could in fact happen quite easily, could lead to more caution in their actions. Therefore it is absolutely crucial to emphasize this, in all of these proposals to change the culture of Intelligence Agencies.

Chapter 10

Leaks

Intelligence agencies are fundamentally opaque, anti-democratic institutions. Unlike in other public bodies, whistleblowing reveals what would *never* otherwise be made public (and in breaking the Official Secrets Act (OSA) 1989, is a crime without a public interest defence). To work in this industry one must accept this secrecy, just as enlisting for military service entails a loss of some basic rights; working for an intelligence agency by necessity curtails individual freedoms.

With no dirt to publicize, nobody can blow the whistle. Ensuring this (tackling the supply of reasons to disclose) requires work — the agency must ensure its employees act ethically and obey the law — and as we all wish to see at least the first of those, this is the only viable option. In practice, there must be management structures for fixing problems as they occur, and the rest of the chapter looks to balance the committment to ethical behaviour with more active leak prevention.

Nonetheless, it is in the public interest and in the interest of the intelligence agencies to put in place a management strategy that prioritises ethical behaviour. The strategy put forward in this report would hopefully increase public trust in intelligence agencies by ensuring that employees are bound to report unethical behaviour to a body which has the responsibility to address these issues. Employees would then ideally have no need to leak this information to the press, and so whistleblowing may be prevented. The strategy increases the role of MPs in making ethical decisions regarding intelligence agencies, and would involve reducing the quantity of classified information whilst heightening measures taken to keep secret that information which does need to remain classified. This display of a willingness to be more transparent in some ways countered by a greater commitment to national security in other ways are intended to make the public feel safer from both security threats and government encroachment on civil liberties. In this section of the report, a two-stage strategy for balancing a commitment to ethical behaviour and preventing leaks that are potentially damaging to national security will be proposed. At each stage, these proposals will be compared with an overview of procedures currently in place at GCHQ.

10.1 Recruitment

The recruitment process plays a fundamental role in an agency's ability to ensure that employees are committed to ethical and discreet behaviour. Currently, GCHQ has stringent nationality requirements for employees () as part of its rigorous seven-stage selection process. Although it is not explicitly stated on GCHQ's website, it seems safe to assume that the internet footprints of candidates are also carefully checked. GCHQ's recruitment process seems to have in place all of the viable filtering processes that could be used to ensure the reliability of candidates. Nevertheless, several adjustments could be implemented to further restrict the possibility of hiring potentially unsuitable candidates. These should have an equal emphasis on both loyalty to GCHQ, and on a commitment to moral integrity and operating within the law:

- **Make specific provisions in the Official Secrets Act (OSA) 1989 allowing (a restricted form of) whistleblowing.**
- **GCHQ should adopt the NSA's strategy of interviewing close confidants of candidates (2012).**

10.1.1 Complaints procedure and regulation

Move to the 'About GCHQ' section, possibly as a figure

Currently the legal framework governing GCHQ is too fragmented. GCHQ has to report to the ISC, a cross-party body which examines the expenditure, administration and policy of the three intelligence agencies in the UK as well as the intelligence-related activities of the Cabinet Office. Two senior judges serve as commissioners (interception of communications, and intelligence services) who have oversight of GCHQ. The organisation has a duty to disclose all information and documents that these commissioners might require, and this duty extends to the IPT as well. The Human Rights Act of 1998 also compels GCHQ to comply with EU law which requires all public bodies to protect citizens' rights under the European Convention on Human Rights.

A consequence of GCHQ's fragmented oversight is that GCHQ has more power than its regulators. Oversight must not be from another intelligence agency (as this just shifts the problem upstream); at the same time, GCHQ must trust its overseers.

find reference

- **Establish an ethics committee comprising MPs on the ISC, strategic management at GCHQ, legal experts and academics.**
- **Retain the cross-party ISC with responsibility for overseeing reports from the Ethics Committee as well as from the Foreign and Home Offices.**

► **Charge the IPT with investigating the Ethics Committee's concerns.**

The ethics committee ensure all practices are ethically acceptable, and that the law is changed where such practices (and their appropriate safeguards) are missing. They submit cases to the IPT for further investigation. The IPT would continue to have responsibility for handling individual cases. Its findings should in turn reveal areas of weakness within GCHQ and the system of oversight, and should therefore be of use to the Ethics Committee.

The commissioners would report their concerns to the Ethics Committee. These commissioners would have access to highly classified information; currently they are both former senior judges.

Diagrammatic representation of proposals

Disciplinary Tribunal — carries out investigations of misconduct on recommendations of Ethics Committee or ISC or Commissioners. Gives advice to Ethics Committee. Works with standards set out by Ethics Committee to enforce disciplinary procedures.

ISC — cross-party committee with responsibility to listen to ethics committee, foreign and home offices, commissioners, MPs, Cabinet, and heads of intelligence agencies

Home Office — commissioners, Secretary of State

Foreign Office — commissioners, Secretary of State

Ethics Committee — ISC members, GCHQ representatives, legal experts, intelligence experts

10.2

Ultimately, the aim of any oversight of GCHQ's activities should be to strictly guarantee compliance with any laws and/or code of conduct. Legality is necessary (albeit insufficient) to the validity of an institution's existence and to public trust in that institution.

Bibliography

URL: http://www.gchq-careers.co.uk/how-to-apply/how-to-apply/nationality-security/

(2012). Last modified: June 18th, 2012 First posted: January 15th, 2009.
URL: http://www.nsa.gov/careers/faqs/index.shtml#atNSA_15

Feynman, R. (2006). *Classic Feynman*. New York, NY: W. W. Norton & Company, Inc. ISBN: 0-393-06132-9.

Lanchester, J. (2013). *The Snowden files: why the British public should be worried about GCHQ*. London, UK.
URL: http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester

Schneier, B. (2008). What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites. *Wired*.
URL: http://www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124?currentPage=all

Schneier, B. (2012). *Liars and Outliers*. Indianapolis: Wiley. ISBN: 978-1-118-14330-8.

Shapiro, J. N. (2013). The Business Habits of Highly Effective Terrorists. *Foreign Affairs*.
URL: http://www.foreignaffairs.com/articles/139817/jacob-n-shapiro/the-business-habits-of-highly-effective-terrorists