Chapter 8

8 Threats and risks

8.1 Introduction

The documents leaked by Edward Snowden provide evidence that GCHQ engages in a very broad range of activities that go well beyond surveillance. Besides bulk collection programmes such as Tempora, as we saw in Part One of this report, there is evidence that GCHQ has exploited weaknesses in Internet security, hacked computers, carried our Denial of Service attacks and has an ongoing programme for the infection of target computers with a variety of malware (See Chapters 4 & 5).

An oft-repeated defence of mass surveillance is that if you have nothing to hide, you have nothing to fear. The implication of this argument is that only the guilty are negatively affected by mass surveillance; for the rest of us, undermining our right to privacy is a small price to pay for protection from terrorist groups, serious criminals and antagonistic foreign powers. But activities that exploit weaknesses in the Internet threaten more than our privacy. They risk serious damage to Internet security, law enforcement and the economy; and are inconsistent with government commitments to promote the UK's digital economy.

Mass surveillance also undermines our ability to exercise our basic democratic rights as neither we nor our MPs have a full picture of what the surveillance services are doing. We have to blindly trust that a secret system of checks and balances is working. But the capacities of the intelligence agencies to monitor and manipulate online behaviours go much further than anything envisaged in the current framework of surveillance regulation. If we allow the intelligence agencies to determine their own legal and policy agenda, there is an imbalance at the heart of our democracy, that could prove highly corrosive. As this section outlines, mass surveillance affects other rights, such as freedom of expression and freedom of association as people feel afraid to express their opinions on controversial matters. Collecting data on the entire population also undermines the presumption of innocence that underpins our legal system.

While the security agencies' data collection aims to support the UK's foreign policy objectives, it is inconsistent with some of our foreign policy commitments, such as the promotion of human rights and the rule of law.

It is probable that the advancement and protection of GCHQ's reputation and abilities is seen by many security employees as core to the overall mission of protecting the UK's international interests through intelligence gathering. Holding the security services to account should not be seen as an attempt to undermine their work but an endorsement of the democratic processes that they are here to protect.

In this section, we outline the threats that GCHQ's programmes create and ask whether Parliament has the information and the mechanisms to balance these threats against the perceived benefits of mass surveillance.

8.2 The threat to democracy

A fundamental difference between a democracy and an authoritarian state is the ability of citizens to hold their government and its agencies to account. This is necessary because the agencies are engaging in activities that would normally be considered illegal and very harmful. They are given highly dangerous powers that can quickly be abused; unchecked they could easily be used to overthrow a government, cause the wrongful arrest of citizens or destroy people's lives for political ends.

Thus, even the sense that agencies are out of control will quickly create a sense of threat among anyone who believes that they might become the next victim. And it is irresponsible to assume that our agencies will never cross the line and interfere with political processes.

The dynamics in any institution can be dangerous. For instance, it can be hard to separate the ends and the means, especially when the ends that are sought are preservation of national security. Equally, most institutions find it hard to separate their own reputation and survival from their mission. We expect this balance to be maintained through the law and through our democratically elected representatives. As we showed in Chapters 6 and 7, neither of these instruments are fit to fully hold the secret services to account, which threatens our democratic balance.

We recognise that there has to be secrecy about the intelligence services' work but there is a difference between operational secrecy and proper oversight. One of the shocking aspects of the Snowden revelations is that British MPs had little idea about the extent of surveillance being carried out. It took a foreign whistleblower for us to find out.

Fundamentally, this is an issue of trust. Since the public cannot directly oversee the work of the intelligence services, then we have to entrust our democratic representatives to do so on our behalf. As we saw in Chapter 7, current oversight arrangements are not sufficient and have been criticised by the Home Affairs Committee[i]. A particular issue is that the ISC is not truly answerable to Parliament. The arrangements are imbalanced and reform is needed if there is to be meaningful parliamentary oversight.

8.3 Protecting against institutional abuse

Without proper accountability, how do we know whether our security services are abusing mass surveillance? We have had to rely on a whistleblower. The sheer scale of surveillance and potential intrusion into individuals' lives can be open to political abuse. If the executive holds the key supervision mechanisms, through appointments, it can weaken the ability to detect when systems are failing or being abused.

Historically, surveillance within democratic countries has been used against human rights organisations, environmental groups, trades unionists and political activists. Surveillance can threaten freedom of speech, freedom of assembly and the political debate expected in a democracy.[ii] The question for today's politicians is whether they can be confident that people or groups are not being targeted inappropriately, and that access to the vast wealth of personal information held by GCHQ and shared with the NSA is not being abused.

Given the secrecy of the security services' activities, it it is difficult to know if abuses are being committed but we have seen how surveillance has recently been used by UK law enforcement. Surveillance was used to target the Lawrence family in order to see if there was information that could discredit their campaign for justice, after what they saw as a botched police investigation of their son's death.[iii] Holding law enforcement and intelligence agencies to account should not be seen as an attack on their mission but an endorsement of the democratic processes that they are here to protect.

An example of how mass surveillance can be abused was shown in reports of NSA employees turning the agency's powerful machinery towards their own love interests[iv]. The activity even got its own tongue in cheek codename among the intelligence community: LOVEINT. According to the agency these constituted the majority of relatively small numbers of wilful abuse. The NSA reported a total of 2776 surveillance violations in the twelve months leading to March 2012[v], although the majority were due to unintended errors. There are no comparable figures available for GCHQ.

8.4 Freedom of expression

Freedom of expression is essential if we are to fully engage in society, debate and challenge ideas and participate in democratic processes. A free media holds governments and the powerful to account. If freedom of expression is threatened, so is democracy.

In 2014, the UK dropped down 3 places to 33rd in the World Press Freedom Index. Reporters Without Borders, who compile the index, cited the destruction of files in The Guardian's offices following the Snowden revelations and the detention of David Miranda under section 7 of the Terrorism Act as some of the reasons for this fall. It noted,

'By identifying journalism with terrorism with such disturbing ease, the UK authorities are following one of the most widespread practices of authoritarian regimes.'[vi]

The threat to media freedom from surveillance itself was exposed in July 2014 when it was revealed that the police had used RIPA to access the telephone records of a Sun journalist in order to identify a whistleblower. In doing so, they bypassed journalistic privilege to protect their sources. Under the Police and Criminal Evidence Act 1984, the police need to get permission from a judge to access a journalist's telephone records in order to identify a source. However, the police do not need judicial or ministerial authorisation for RIPA requests, merely approval by a senior officer. A Code of Practice now covers journalistic communications but still doesn't require independent authorisation.

After other high profile cases and pressure from media groups, the Interception of Communications Commissioner launched an inquiry into the acquisition of communications data by police forces to identify journalistic sources, which concluded that: "judicial authorisation must be obtained in cases where communications data is sought to determine the source of journalistic information."[vii] Despite this, potential whistleblowers, who have information that is in the public interest, may be deterred from speaking to journalists if they fear that they can be identfied through surveillance.

This does not cover the surveillance of journalists by GCHQ. According to a Guardian report, documents leaked by Snowden show that GCHQ collected and shared the emails of journalists working from international news organisations, including the BBC, the New York Times and Reuters[viii].

Writers have also expressed concerns about surveillance. A global survey of writers by PEN America on the impacts of mass surveillance shows that "the levels of self-censorship reported by writers living in democratic countries are approaching the levels reported by writers living in authoritarian or semi-democratic countries" [ix].

We need to ask whether we are likely to become a target or person of interest if, for example, we have legitimate but fringe political views or join a demonstration? The police believe so, and the Supreme Court has given them blanket authority to collect information on innocent people engaged in protests[x]. Do we need to exercise caution in what we say? Many people seem to think the answer is yes.

8.5 Confidential and privileged communications

As well as journalists, there are a number of other professions who need to be able to communicate confidentially, including doctors, clerics, lawyers and politicians.

The right for lawyers to communicate confidentially with their clients is a fundamental human right, recognised by common law and by the European Court of Human Rights. It is seen as essential in ensuring that people have the right to a fair trial. In February 2015, the government admitted that its policies on how the security services handle privileged communications between lawyers and their clients had breached human rights law.[xi]

MPs' communications are protected by the Wilson Doctrine,[xii] which prohibits the wiretapping of MPs and Peers' phones. However, government ministers have stated that the Wilson Doctrine only applies to the content of communications, and not to metadata.[xiii] As we have seen above metadata can be as revealing as the content of communications. Caroline Lucas MP and Lady Jones of Moulescoomb have raised a formal complaint[xiv] at the Investigatory Powers Tribunal, asking for a declaration that the interception of her communications – including confidential correspondence with constituents – has been prohibited. In November 2014, the Justice Secretary Chris Grayling apologised after it was revealed that confidential telephone calls between MPs and prisoners had been recorded[xv].

Grayling said that the monitoring had been accidental not intentional, which illustrates how if systematic surveillance is in place, it is difficult not to breach confidentiality.

It is nearly impossible to see how a system of mass collection and analysis can be engineered to fully protect categories of privileged communications. The processes for accessing these communications are designed to allow access for law enforcement and other agencies with little external supervision – for example, the police and other organisations sign off RIPA requests internally.

Without subjecting all requests to limitations on both collection and external supervision, abuses are hard or impossible to control. This could easily undermine trust in political and legal processes, especially among groups who feel they may be subjected to unfair attention.

8.6 Discrimination, profiling and social cohesion

Mass surveillance programmes undermine everyone's right to privacy. But the effect of surveillance is not simply a minor temporary discomfort. Many psychological studies have found negative effects of surveillance, breeding conformity, homogeneity and mistrust, which can undermine democratic authority[xvi].

Surveillance is supposed to help protect us from crime but it can make many people feel less safe. It also undermines social cohesion, which is necessary for security. Mass surveillance could disproportionately generate loss of trust and confidence among particular groups at risk of disaffection. According to research by the Equalities and Human Rights Commission, British Muslims already appear to feel disproportionately targeted by counter-terrorism measures. Complaints include the way Muslims are treated when travelling through airports and the existence of CCTV programmes such as Champion in Birmingham, which focused on Muslim neighbourhoods.[xvii] Pervasive monitoring of communications can only foster further mistrust.

In the US, it was revealed that the NSA had been monitoring the communications of respected American Muslim leaders. They included Faisal Gill, “a longtime Republican Party operative and one-time candidate for public office who held a top-secret security clearance and served in the Department of Homeland Security under President George W. Bush”.[xviii] Documents obtained by the Huffington Post revealed that the NSA also monitored the sexual habits of law abiding radical Muslims hoping to be able to discredit them[xix] by exposing the inconsistencies between their private and public personas.

8.7 Threats to the security of the Internet

GCHQ's program to 'Master the Internet' is based on attempting to create full access to everything that happens online anywhere and everywhere. Traffic data is collected and analysed as a matter of fact. Internet security mechanisms, such as encryption, that protect the privacy of users' information create obstacles for the agency's mission. Its response has been to increase access by breaking or circumventing these technologies.

The apparent confirmation that the NSA and GCHQ have been working to undermine widely used technologies and standards has deeply concerned security specialists and Internet businesses. These revelations have created a drive towards the strengthening of the privacy and security of Internet communications for the general population. The World Wide Web Consortium (W3C) – the technical network in charge of keeping the Internet running – has reacted against what they perceive as a fundamental threat. W3C now have a working group dedicated to modify the architecture of the net to prevent what they call "pervasive monitoring" by security services.[xx]

Major Internet companies are now bringing security features that will have an impact on the capacity of the security services to access their customers' information. Yahoo and Google are preparing to offer end-to-end encryption for emails, as in the words of one of their security consultants: "privacy is much more effective as a selling point than it used to be".[xxi] Messaging app Whatsapp, owned by Facebook has also started to scramble its customers' messages[xxii].

Most software engineers believe that people must be able to choose their own software and security measures, and it is highly undesirable to compromise equipment and software, because it inevitably creates bugs and potential exploits that are available to criminals as well as security agencies.

8.8 Threats to personal security through curbs on privacy technologies

There is a backlash from the security services against the spread of secure technologies, with calls to curb their use, or include backdoors or deliberate security loopholes. FBI Director James Comey has been quite clear:

"There will come a day—well, it comes every day in this business—when it will matter a great, great deal to the lives of people of all kinds that we be able to, with judicial authorization, gain access to a kidnapper's or a terrorist's or a criminal's device," he said Thursday. "I'd hate to have people look at me and say, 'Well, how come you can't save this kid?'"[xxiii].

The response of the UK Prime Minister, David Cameron, to the Charlie Hebdo attacks has been to promise new legislation after the elections to ensure that there are no "means of communications" which the security services "cannot read"[xxiv]. Cameron's apparent calls to limit encryption were strongly criticised by security experts. Blogger and computer security expert, Graham Cluley, said: "Cameron is living in cloud cuckoo land if he thinks that this is a sensible idea, and no it wouldn't be possible to implement properly."[xxv]

Panics about access to strong cryptography have happened before. During the 1990s the so-called Crypto Wars saw demands for backdoors and keys to be deposited in escrow.[xxvi] Eventually cryptography became widespread and the basis for online trust, enabling online commerce and secure services.

Apple encrypts iPhones and iPads in a manner that makes it impossible for the company to hand the key to law enforcement agencies. In their Privacy statement, they state:

"On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."[xxvii]

Privacy enhancing technologies are used for many legitimate purposes, including preventing serious human rights violations. For example, Syrian dissidents use Tor to protect themselves from the Assad regime.[xxviii] If the UK restricts the use of Tor or strong encryption, the authorities of these countries would be legitimised to take similar actions. In addition, Tor relies on peer-to-peer collaboration to provide anonymity and bandwidth.[xxix] Restrictions on Tor usage in the UK could have a direct negative impact on citizens of non-democratic states.

The use of strong cryptography specialist tools may become increasingly common within high risk groups requiring protected communications – such as human rights workers, journalists, mental and sexual health professionals, patent attorneys, technology innovators, and so on. There is no easy answer to the conundrum this presents for legitimate law enforcement, and certainly not from a technological standpoint. However police detective work has proved successful in dismantling sophisticated criminal enterprises that rely on secure technologies, such as the Silk Road marketplace for illegal goods[xxx]. This suggests that encryption is unlikely to be a silver bullet to avoid detection as it is sometimes presented.

8.9 Threats to secure technology from targeted intrusion

Targeted intrusion is when security agencies try to decide how to access either networks or an individual's equipment to gain knowledge about them. As we can see from the leaked documents this includes targeting of innocent people and organisations.

First, an agency needs to know a means of gaining access, which means actual knowledge of a problem with publicly used equipment or software. They must decide whether to report the problem to a company. If the bug is not reported, users of that device or programme remain vulnerable to attacks, globally, from anybody who finds the same problem. If the problem is rare, and surprising, and therefore perhaps less likely to be found by a third party, the agency may deny security researchers knowledge about new kinds of problems they need to look out for. If it is a common kind of problem, the exploit is likely to be found by others, and exploited for harmful and unpredictable purposes. Either way, there is a likely cost to the "cyber security" of individuals and businesses.

It should be clear that using exploits for access to equipment and devices carries many risks. No doubt the agencies understand this but feel they have no choice. How then do they make a reasonable risk assessment, given that the problems they fail to report may exist in equipment and software used by millions of people scattered across the globe? Does potential damage to citizens in allied countries, or indeed any country, count, or do we only worry about damage to UK citizens? Who is checking to decide if this balance is struck in a reasonable manner?

A second aspect of this problem comes when GCHQ decides that it needs access to networks, or perhaps encryption technology such as certificated used in SIM cards. In these cases, GCHQ may make a decision to compromise a foreign network (such as Belgacom in 2010[xxxi]), a foreign company (such as Dutch firm Gemalto in 2010-11[xxxii]) or compromise a network of computers that are themselves not targets, in order to gain unauthorised access to other computers in the future.

To the people whose equipment, networks or security are compromised, there are direct impacts on their business. These include having to remove malware originating from GCHQ if they are found; protecting from future attacks; a loss of trust from customers; liability for leaking customer data; and in the meantime, they may find that the compromises created by GCHQ have caused further unknown security problems that they could not anticipate, as security relies on understanding the software running on your system and what precisely it does.

The consequence of GCHQ's attacks on foreign networks or equipment are, to the owners, much the same as any criminal breaking in. The methods and costs of dealing with such invasions are the same. It will appear lawless, irresponsible and unaccountable; it is likely to create a pervading sense of insecurity among the operators; and it will be extremely hard for them to hold GCHQ to account for their actions and the costs our agencies may impose on them.

How then should GCHQ evaluate their actions? Would a course of co-operation with foreign partners be preferable, or is this on occasion impractical? If it really is impractical, how does GCHQ decide that the benefits of their invasion of a network or public equipment outweighs the costs to overseas companies and their customers, often in allied countries? Or is it because the benefits and costs to the UK are all that count?

These questions arise because SIGINT techniques have moved from telephony to ubiquitous Internet networks. They have been aided by Internet technologies that most computer engineers feel are not well-designed for security, but promise global access to anyone including our agencies. The breadth of the consequences reflect the breadth of the technology and its user base.

It is going to be a significant challenge for Parliament, the executive and judges to understand the threat as it depends on who GCHQ is targeting, understanding the precise methods, the computer security risks that are generated and the potential social and economic consequences to the intermediaries whose equipment and software is invaded or exploited. There is a significant risk of failing to hold the decisions of GCHQ to account, despite the very high risks that they are running.

It is also worth noting that GCHQ's CESG (Communications-Electronics Security Group)[xxxiii] have responsibility for Information Assurance in government – that is removing security problems and ensuring that systems are secure – while GCHQ as a whole must ensure that SIGINT has the capability to use the same kind of problems to break into other people's systems. There is a case to separate these functions and a high potential for conflict of responsibility.

8.10 Threats to Internet governance

The UK has been at the forefront of the promotion of efforts to maintain the international multi-stakeholder model of Internet regulation. Other countries, including China and Russia, favour a more top-down approach which would allow them to impose controls on Internet infrastructure that falls under their national borders. For example, Russia has recently announced plans for a 'kill switch' capable of cutting the country off from the global Internet.

At the Seoul Conference on Cyberspace, former Foreign Secretary William Hague said:[xxxiv]

"(...) On the other side are countries calling for an international legal framework for the Internet that would enable governments to exercise exclusive control over the Internet's content and resources.

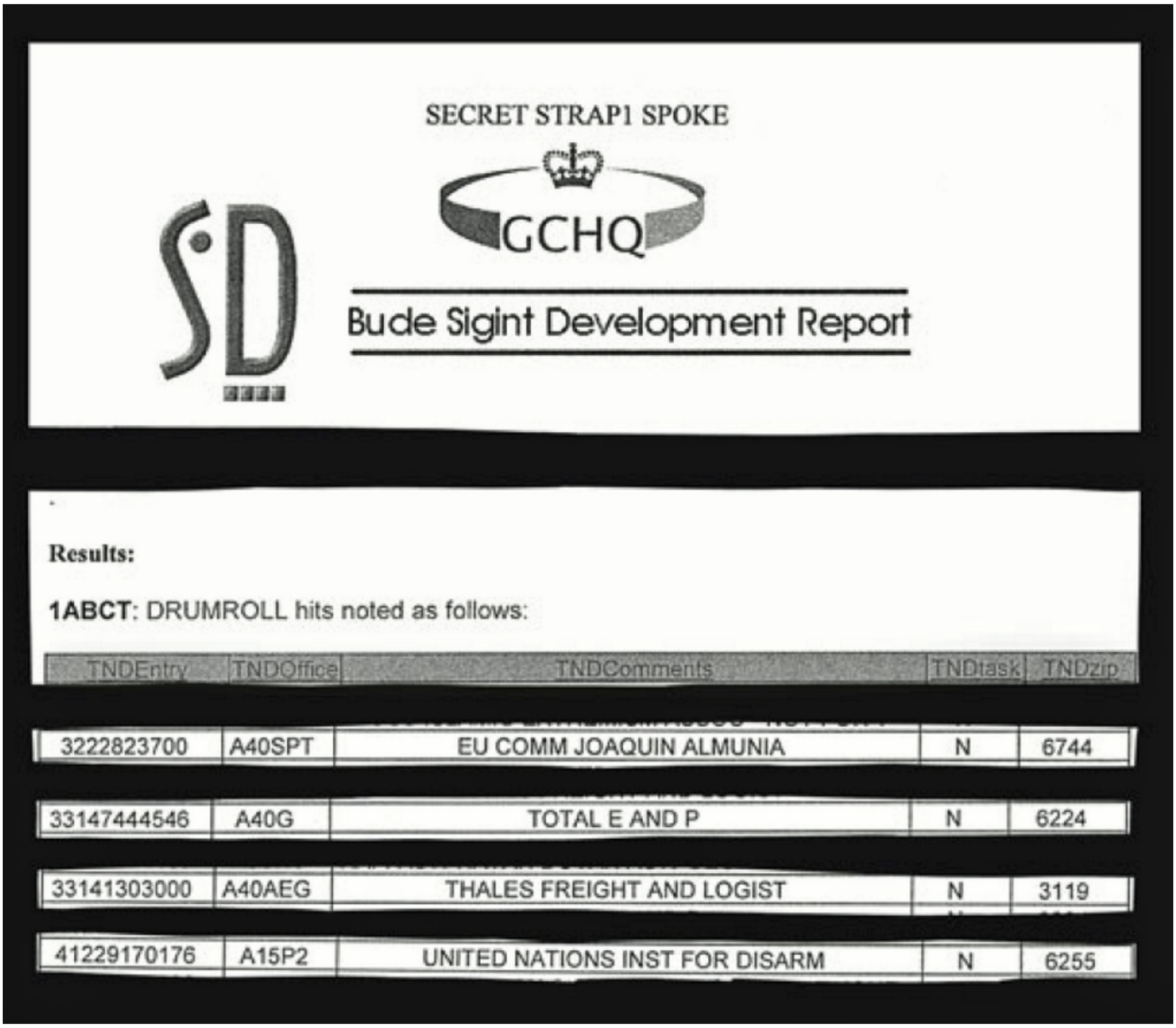
I am convinced that placing the controls of cyberspace entirely in the hands of governments would be a drastic error that would have profound social and economic consequences."

GCHQ's work undermines the stated UK position on Internet regulation and risks legitimising the behaviour of states that openly want to impose restrictions on Internet infrastructure. Any review of surveillance should consider the damage that mass surveillance inflicts on the models of Internet regulation that have so far greatly benefitted the UK.

8.11 Threats to UK's foreign standing

The 2010 UK National Security Strategy[xxxv] states that it is in Britain's national interest to promote the rule of law and human rights abroad because it makes us safer. But this is undermined by the disproportionate interference with the privacy and security of millions of people under the cover of secret intelligence sharing pacts. In addition, revelations on mass surveillance can be expected to have weakened our standing with allies and created questions about our close relationship with the US.

Documents seen by the Washington Post show that GCHQ and the NSA had been targeting a broad range of foreign interests[xxxvi]. Some of the activities focused on ally governments, such as Turkey[xxxvii], which is partly expected, but revelations that the GCHQ had spied on Joaquin Almunia the EU official charged with trade deals caused particular anger.



SECRET STRAP1 SPOKE

GCHQ

Bude Sigint Development Report

Results:

1ABCT: DRUMROLL hits noted as follows:

TNDEntry	TNDOffice	TNDComments	TNDtask	TNDzip
3222823700	A40SPT	EU COMM JOAQUIN ALMUNIA	N	6744
33147444546	A40G	TOTAL E AND P	N	6224
33141303000	A40AEG	THALES FREIGHT AND LOGIST	N	3119
41229170176	A15P2	UNITED NATIONS INST FOR DISARM	N	6255

The Guardian newspaper published documents showing how GCHQ had spied on allied diplomats at the 2009 G20 meeting in London[xxxviii]. The agency obtained calls and emails from smartphones, such as Blackberries; and set up fake Internet cafes in order to gather information. Intelligence was fed to ministers to be used during the negotiations. Similar revelations that GCHQ spied on delegations at climate talks are being investigated by the UN[xxxix].

There is evidence that agencies target elected politicians in allied countries. A senior US official admitted that the NSA was "probably" spying on members of congress and their staff[xl], and the agency refused to categorically deny this was the case.[xli] In addition to widespread reports of the tapping of Angela Merkel's phone,[xlii] German media reported that the NSA had also spied upon European institutions,[xliii] which generated widespread complaints from policymakers across Europe. We know less about GCHQ's activities in this regard, although the GCHQ hacking of Belgacom for instance, may lead to a suspicion that we have aided NSA access to the EU institutions' data.

These kind of activities have been widely documented in the past and should come as no surprise, they are the traditional bread and butter of spy agencies. But the gigantic mass spying capabilities of the Five Eyes places them in a new context.

8.12 The UK's relationship with the US

The high level of integration of the UK's surveillance apparatus with US agencies has implications for our foreign policy. While the UK perhaps benefits from a 'special relationship', it is highly dependent on the US for the NSA's technology and data. Can we expect the USA to indulge the UK by allowing us to rely on their data and resources to pursue a contradictory goal?

This exacerbates the difficulties the UK may have separating its own strategic interests from those of the USA. We would expect that similar questions will be raised by European partners. They too will want to consider how this shared intelligence infrastructure affects the UK's foreign policy calculations.

The NSA could have access to compromising personal information of politicians and journalists from any country, as we saw above including the UK. We might speculate at the leverage they could exercise, or the implicit threat this may create. If there were a crisis in the relationship between the UK and the USA, what risks would this pose? Could the UK democratically decide to stop its mass surveillance programmes unilaterally?

While these may be threats that politicians are prepared to accept, the very least that is required is a thorough public discussion of the consequences and how to manage issues that arise. Compared to our membership of NATO for instance, it has been little discussed, even in terms of what really underpins our 'special relationship' with the USA.

8.13 Drone strikes

"We Track 'Em, You Whack 'Em." (NSA Geo-location unit's motto)[xliv]

British involvement in drone strikes would appear to be in direct conflict with our stated aim of promoting the rule of law and human rights abroad.

Concerns have been raised about the involvement of GCHQ in drone strikes since 2010[xlv]. A legal opinion by a respected QC found that GCHQ workers could be complicit in war crimes if they helped strikes in undeclared conflicts, such as Yemen[xlvi]. In 2011 the relatives of man killed by drones in Afghanistan took GCHQ to court over its role in the strikes. The case was eventually thrown out by the Court of Appeal without full consideration, because it would imply passing judgement on the sovereign acts of the US[xlvii].

Data analysis can provide the accurate location of a device, but there is no guarantee that the device is in the possession of the person of interest. This can lead to the killing of the wrong person. In addition there are questions about whether remote killings outside the theatre of operations fall within the definition of fighting "combatants". Several human rights organisations are calling on the US government to be more transparent about drone use.[xlviii]

There is widespread evidence that information from the NSA is used in drone strikes resulting in the deaths of both targets and innocent civilians.[xlix] This has generated growing calls, including from the former head of GCHQ[l], for the UK to disclose the guidelines governing when the UK may share intelligence to help locate individuals on the US 'kill list.'

Tom Watson MP, Chair of the All Party Parliamentary Group (APPG) on Drones, has called for: "an informed public debate about this new era of war-making technology. Parliament should know about our own lethal operations and the various ways we support the drone programme of the United States – shared communications systems, shared data, shared assets and exports. All future action has to comply with our own understanding of human rights and the laws of war."[li]

8.14 Threats from the militarisation of cyberspace

The line between surveillance capability and offensive weaponry has been crossed by the development of malware and Denial of Service attacks. Malware is installed to control a computer or network. It can however be used either to harvest information or to damage or switch systems off.

This is recognised in the Snowden documents which outline the weaponisation of our surveillance capabilities. For Parliament this raises a very serious question: is it legitimate to have secret capabilities to damage foreign powers? Are we incentivising others to attempt to control our systems too? At what point should our elected representatives seek a public debate about entering into an entirely new field of war, which would inevitably be more likely to target less protected civilian systems than combatants?

There are concerns about the growing militarisation of cyberspace. This trend is mainly characterised by an excessive focus on the strategic and military aspects of cyber security, which according to policy experts "centres too strongly on national security measures instead of economic and business solutions, and wrongly suggests that states can establish control over cyberspace."[lii]

The UK has so far argued that cyberwarfare would be regulated by existing international instruments. However, this approach denies us the serious discussion about the moral and ethical issues that arise from these capabilities, especially surrounding their invisibility, lack of acountability and unknowability.

8.15 Threats to UK business and innovation

Mass surveillance can lead to a loss of consumer confidence. This a particularly important issue for the UK, which is a world leader on E-commerce, with sales of £492 billion in 2012, accounting for 18% of business turnover.[liii] In 2014 some 74% of UK adults used the Internet to make a purchase.[liv]

Industry insiders, such as Martin Sorrell chief executive officer of WPP Group, have raised concerns about the impact on consumers of this new awareness about mass surveillance.[lv] An Ipsos Mori poll published in February 2014 found that "68% of Britons are concerned about the way information is collected about them by government, and even more – 76% – are worried about information collected on them by companies".[lvi] These increased levels of concern about Internet companies is repeated in other polls,[lvii] with one possible explanation being that awareness of government surveillance contributes to a generalised loss of confidence on "the Internet", which is then identified with well known brands.

A recent US survey found that 47% of respondents have changed their online habits due to the activities of the NSA, with some 26% saying they have reduced their online banking and shopping.[lviii] If this trend is confirmed in the UK, with our higher levels of online commerce, it could have serious economic consequences.

A survey of ICT decision makers in France, Germany, Hong Kong, the United Kingdom and the USA found that 88% are changing their buying behaviour due to surveillance revelations. 82% agree with Angela Merkel's proposals for separating European data networks.[lix]

US Internet firms are very concerned at the loss of business. A 2013 report estimated that the US cloud industry could lose between $22 and $35 billion over the following three years as a result of the recent revelations.[lx] At face value, this could be perceived as a positive effect for UK and European businesses. But analysts Forrester quickly pointed out that it is not just a problem for American companies: "a greater understanding of this surveillance picture could have a chilling effect on all hosting and outsourcing services (not just cloud computing) in many countries."[lxi]

8.16 Externalities and cost benefit analysis

Throughout this report we have discussed the complexity of assessing the risks, costs and benefits of any of these mass surveillance activities. Above, we have expanded on some of the specific risks that GCHQ is running, or creating for third parties, such as companies, networks and their users.

The leaked documents appear to show an approach where the ends justify any means, with little regard for collateral damages. Even in the case of foreigners, and especially where innocent intermediaries are effectively targets, GCHQ needs to be highly focused in their approach, rather than finding broad-brush means of data acquisition. It is unclear that hacking can be seen to be targeted, when looking at GCHQ's actions to access bulk data at Belgacom, to steal Gemalto's encryption keys in bulk, or to siphon off Google and Yahoo's data from their private cables.

From a basic reading of the published Code of Practice for Equipment Interference, we find it hard to believe that these external risks - rather than internal operational risks - are properly considered. Furthermore, it appears to us that 'lack of access' to data is seen as the primary threat, on the basis that not having information would mean that threats may not be detected.

The new risk models we discussed in Chapter 3 around the handling of the possibility, instead of the probability, of catastrophic events lead the agencies to justify any intrusion, because without an intrusion there would be a risk. Rather, specific and known threats need to be measured against specific, targeted interference.

In addition, the agencies appear to have fallen in with the zeitgeist – well captured by scholars such as Evgeny Morozov[lxii] – that data will solve everything, but data creates new problems.

There are some real issues driving mass surveillance. The move from communications lines for phone and telex made it easier to engage in targeted surveillance. When you move to Internet packets it can be harder to isolate individuals without looking at the data stream in which these flow. But wholesale global surveillance is a disproportionate response.

Politicians and oversight need to be extremely careful about risk assessment and must ensure that they have sufficient expertise on hand to understand what risks exist, how they are managed and whether the risk assessments are reasonable. Risk assessment may be the critical component for external oversight to examine, especially in relation to "equipment interference".

8.17 Effectiveness of surveillance

The excessive secrecy currently surrounding national security and surveillance makes it difficult to provide proper public accountability for the services' effectiveness.

Since the Snowden revelations, both the US and UK agency chiefs have argued that mass surveillance is necessary to prevent terrorist attacks. In November 2013, Andrew Parker, Director General of MI5, told the ISC that the police and intelligence agencies had disrupted 34 terrorist attacks since the 7/7 bombings in London.[lxiii] The NSA claimed its surveillance had prevented 54 plots but during Congressional hearings in 2003, NSA Director Keith Alexander acknowledged that they were not all plots and only 13 had connections to the US.[lxiv]

Undoubtedly, the intelligence services need surveillance powers but, privacy concerns aside, there is no evidence that increasing powers to monitor every citizen's communications would prevent every terrorist acts.

The report by the ISC on the murder of Fusilier Lee Rigby in Woolwich showed that his killers, had been known to the intelligence agencies prior to the attack, appearing in seven different investigations. Despite the report showing a catalogue of errors by all agencies involved, and even with some access to secret material, the committee relied on the agencies' own assessments, and concluded that only Facebook could have possibly prevented Rigby's murder[lxv]. The report called for more co-operation between tech companies and the security services. But even former Head of MI6, Richard Barrett questioned whether it was fair or realistic to expect Facebook to report terrorist activity, given the volume of posts on Facebook each day[lxvi]

More recently in France, despite extensive surveillance systems and previous knowledge of the suspects, the French security services were unable to prevent the murders at the Charlie Hebdo offices and at a Jewish supermarket.

Surveillance is not just about law enforcement and anti-terrorism, it is also part of the strategic intelligence process. The massive expansion of Internet surveillance appears to have had a limited effect.

In any case, cost benefit analysis and risk assessments are critical to democratic accountability. Explaining how these conclusions are reached must be put to the public in a much more sophisticated manner than the prime minister reminding the public that he would not wish to have denied a surveillance power that might have prevented an incident from occurring.

8.18 Conclusion

The threats posed by GCHQ's activities are much wider than often supposed. What is very clear is that they touch everyone's lives, both from the angle of personal liberty and corrosive effects upon our democratic culture, and in relation to the potential costs to personal security and business.

It is unclear that Parliament and the executive have fully understood these threats. This is understandable, but must be rectified. A robust debate about the legitimacy of techniques that we have learnt about is required. This includes mass surveillance and analytics, but stretches much further than that.

Politicians need to be honest about the debate: there may be no easy answers to some questions, GCHQ may not always be striking the right balance, and it may not be possible to fully meet the desires of state security agencies while also maintaining and enhancing personal and business security. So far it has been more common to hear voices blaming the messenger, in the shape of the Guardian or Snowden, than to find people trying to understand the consequences of what is taking place.

The democratic threats are very real, and need to be dealt with thoroughly by Parliamentarians, as the custodians of our freedoms. Threats to our legal system are also fundamental and cannot easily be brushed aside.

Threats to social cohesion may take some time to be felt and recognised. It will be all to easy to underestimate them, only to find they cause strategic difficulties at a time when it has become too late to rectify.

Threats to technology and Internet security will be very challenging for Parliament, the executive and any judicial oversight that might be applied. Understanding these problems requires independent computer security advice at all levels, and access to the precise techniques and technologies in order to evaluate the risks. The risks are also widespread and consequences will be felt beyond our borders.

The corrosion felt in consumer and business confidence, and the changes to their practices and choices, is appreciable. Indeed, accusations of the parts of the Internet "going dark" probably owe more to business employing routine encryption of data in transit than to criminals changing behaviour. Yet these are highly rational and reasonable changes to protect against very normal threats such as criminal behaviour.

Appreciation of these shifts in business behaviour and the advantages of increased personal security is paramount if we are to avoid further risks including calls for weaker encryption.

Policy makers need to be alert to a very real tension between personal and systemic security, which relies on secure computer, software, networks and encryption techniques; and the desires of national security agencies to maintain insecurities in computers, software, networks and encryption. There will sometimes be no easy answer, but we need to be clear that national security wishes simply do not trump the need for systemic security. It is illegitimate to attempt to deliver surveillance capacity by maintaining collective insecurity.

Many of the threats we have discussed have very real economic implications. They add up to much more than just the result of a few people leaving Facebook or Google losing some advertising revenue. Rather we are witnessing significant and costly changes to computer security, encryption technologies. Many cyber security experts will be saying that this is about time too. But the costs of having to protect against adversaries as sophisticated as GCHQ should not be underestimated; and the costs of being their victim while acting as a mere technology provider are not just financially high, but also risk being very unfairly imposed. Cost benefit analysis and risk models are critical for oversight. There is little discussion of these issues, yet they are fundamental to any understanding that Parliament may have.

When assessing the results of GCHQ's highly developed and extensive programmes, we should be alert to their ability to over reach, posing risks to their efficacy over time. This has, as we noted, already been counter-productive in some areas of foreign policy, especially where advocating for human rights abroad. It has an impact on our allies and strategic choices, restricting our manoueverability through tight arrangements with the NSA. It could also undermine law enforcement domestically, especially if and when things go wrong in public. The breadth of security programmes, and the numbers of people who are touched by data collection, use of equipment or computer programs that may be compromised, the numbers of companies whose networks may have been invaded, means that oversight has almost certainly lost sight of the detail required to mitigate the threats.

i Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 157, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

ii http://www.defendtherighttoprotest.org/supreme-courts-catt-judgment-ignores-reality-of-surveillance-and-seriously-undermines-privacy-protest-rights/

iii http://www.theguardian.com/uk/2013/jun/23/stephen-lawrence-undercover-police-smears

iv http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/

v http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

vi http:/http://rsf.org/index2014/en-eu.php/en-eu.php

vii http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf

viii http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post

ix http://pen.org/global-chill

x https://www.supremecourt.uk/decided-cases/docs/UKSC_2013_0112_PressSummary.pdf

xi http://www.bbc.co.uk/news/uk-31526737

xii https://en.wikipedia.org/wiki/Wilson_Doctrine

xiii http://www.theyworkforyou.com/search/?q=%22wilson+doctrine%22*

xiv http://www.theguardian.com/uk-news/2014/may/04/greens-legal-challenge-gchq-surveillance

xv http://www.theguardian.com/society/2014/nov/11/prisoners-phone-calls-mps-monitored-grayling

xvi http://www.theguardian.com/science/head-quarters/2013/aug/26/nsa-gchq-psychology-government-mass-surveillance

xvii http://www.equalityhumanrights.com/sites/default/files/documents/research/counter-terrorism_research_report_72.pdf

xviii https://firstlook.org/theintercept/2014/07/09/under-surveillance/

xix http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html

xx https://www.w3.org/2014/strint/

xxi http://www.forbes.com/sites/kashmirhill/2014/08/07/yahoo-end-to-end-encryption/

xxii https://whispersystems.org/blog/whatsapp/

xxiii http://www.mercurynews.com/business/ci_26614294/law-enforcement-grapples-apples-enhanced-encryption xxiv http://www.bbc.co.uk/news/uk-politics-30778424

xxv http://www.theguardian.com/technology/2015/jan/13/david-cameron-encrypted-messaging-apps-ban

xxvi http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

xxvii https://www.apple.com/privacy/government-information-requests/

xxviii Eissa, T., & Cho, G. (2013). Internet Anonymity in Syria, Challenges and Solution. In K. J. Kim & K.-Y. Chung (Eds.), *IT Convergence and Security 2012 SE - 21* (Vol. 215, pp. 177–186). Springer Netherlands. doi:10.1007/978-94-007-5860-5_21

xxix Running a Tor relay, bridge, exit or hidden service (http://www.bsdnow.tv/tutorials/tor)

xxx http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/

xxxi http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

xxxii http://www.reuters.com/article/2015/02/25/us-gemalto-cyberattack-idUSKBN0LT0MW20150225

xxxiii http://www.cesg.gov.uk/Pages/homepage.aspx

xxxiv https://www.gov.uk/government/speeches/building-a-new-international-consensus-on-the-future-of-cyberspace

xxxv https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty

xxxvi http://www.washingtonpost.com/world/national-security/nsa-gchq-targeted-broad-spectrum-of-foreign-interests-including-allies-aid-agencies/2013/12/20/b44f9314-6992-11e3-8b5b-a77187b716a3_story.html

xxxvii http://cryptome.org/2014/08/nsa-gchq-spy-turkey-der-spiegel-14-0831.pdf

xxxviii http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits

xxxix http://www.theguardian.com/environment/2014/nov/03/un-investigate-wikileaks-claims-uk-spies-infiltrated-climate-talks

xl http://www.nationaljournal.com/technology/feds-nsa-probably-spies-on-members-of-congress-20140204

xli http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/04/the-nsa-refuses-to-deny-spying-on-members-of-congress/

xlii http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

xliii http://www.spiegel.de/international/europe/eu-officials-furious-at-nsa-spying-in-brussels-and-germany-a-908614.html

xliv http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

xlv http://www.foxnews.com/world/2010/07/25/uk-spy-agency-aids-controversial-targeted-killings/

xlvi http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf

xlvii http://www.brickcourt.co.uk/news/detail/drones-challenge-barred-by-act-of-state-doctrine

xlviii http://www.hrw.org/news/2014/04/02/joint-statement-support-targeted-lethal-force-transparency-act

[xlix] https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/

[l] http://appgdrones.org.uk/wp-content/uploads/2014/08/Rt-Hon-Philip-Hammond-MP9-FINAL-3.pdf

[li] http://www.tom-watson.co.uk/2014/03/drones-report-we-need-an-informed-public-debate/

[lii] http://www.ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf

[liii] http://www.neighbourhood.statistics.gov.uk/HTMLDocs/dvc166/index.html.

[liv] http://www.ons.gov.uk/ons/rel/rdit2/Internet-access---households-and-individuals/2014/sty-digital-day-2014.html

[lv] http://www.theguardian.com/media/video/2014/apr/02/martin-sorrell-nsa-revelations-consumers-video

[lvi] http://www.ipsos-mori.com/researchpublications/researcharchive/3342/Three-in-four-Britons-are-worried-about-companies-collecting-information-about-them.aspx

[lvii] http://www.tnsglobal.com/sites/default/files/whitepaper/TNSBMRB_POMDataTables2014Feb03.pdf

[lviii] http://www.welivesecurity.com/2014/04/02/harris-poll-nsa-revelations-impact-online-shopping-banking/

[lix] http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf

[lx] http://www2.itif.org/2013-cloud-computing-costs.pdf

[lxi] http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

[lxii] http://www.evgenymorozov.com

[lxiii] http://www.theguardian.com/uk-news/2013/nov/07/mi5-chief-34-uk-terror-plots-disrupted

[lxiv] https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible

[lxv] https://www.openrightsgroup.org/ourwork/reports/isc-report-on-woolwich-attack-gets-its-maths-wrong

[lxvi] http://www.bbc.co.uk/news/uk-30206359