# <sup>7</sup> Holding our intelligence services to account

#### 7.1 Introduction

Holding the security services to account should not be seen as an attempt to undermine their work but as an endorsement of the democratic processes they are here to protect.

Proper oversight of these programmes is made almost impossible by the refusal of the government to acknowledge their existence. It is still unclear who - in any of the branches of government - knew about the existence of mass surveillance programmes prior to the Snowden revelations. In October 2013, ex-cabinet minister Chris Huhne confirmed that neither the Cabinet nor the National Security Council had been told about the TEMPORA programme.<sup>i</sup>

The structures for overseeing the security services are not designed to ensure that the agencies are truly democratically accountable. Instead, the agencies are accountable to the executive of the day, with some limited oversight by handpicked Parliamentarians.

As we saw in the last chapter, the de facto powers and capabilities of the security services go considerably beyond the legal framework. This is in part due to the growth of technologies and techniques that make mass surveillance possible. The scale and reach of programs is much larger than that enabled by older communication technologies, such as phones, faxes or telegrams. The trend for greater use of surveillance techniques with the potential to touch ever greater numbers of people should itself be a catalyst for increased scrutiny and oversight. The complexity of the problems, for example, the use of computer exploits, requires ever greater expertise if the accountability processes are to work.

As we have shown in the previous chapter, the agencies appear to be exploiting loopholes in the law. These do not seem to have been detected by Parliament and have not been accompanied by demands for greater powers of oversight.

There is a tension between transparency over capabilities and the need for operational secrecy. The balance between these is struck differently in other countries, including the USA, where it is accepted that capabilities must be publicly disclosed and discussed. In the same way that we are happy to discuss Trident and the nuclear deterrent, the public should be allowed to consider the implications of mass surveillance.

In a democracy, the mechanisms for oversight need to be independent, and capable of understanding, explaining and restraining the activities and capabilities of the agencies. Public trust can be built by more transparency regarding secret service activities and capabilities, and evidence that they have been held accountable if and when they overstep the mark.

Public trust has been undermined by the sense that only whistleblowers have been capable of telling the public the truth about agency programs and powers; that oversight bodies did not really know about these programs; and the apparent defence of the agencies by the same oversight bodies when allegations have been made. This does not suggest that oversight bodies are independent or restraining the activities of the security services.

An additional problem is the international collaboration of the agencies, mainly between GCHQ and the NSA. As noted in the previous chapter, classified bilateral and multilateral arrangements are beyond the supervision of any independent authority – making it almost impossible to assess whether or not they are illegal.

The government has published a "roadmap" that sets out the regulation of surveillance in the UK<sup>ii</sup>, which is very useful but incomplete, as it leaves out parliamentary oversight. The agencies are trying to portray themselves as more open, with public facing websites and revealing the identities of some of their senior staff. While these are clearly moves in the right direction, they do not go far enough.

This chapter looks at the mechanisms provided to create oversight, including the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Intelligence and Security Committee. Individuals can use the Investigatory Powers Tribunal to challenge possible surveillance, but can neither hear all the evidence nor challenge the decisions of the court. We also look at the issue of intercept evidence, and how preventing its use in court further limits accountability. Finally, we note the reviews taking place in response to the Snowden revelations.

'We do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies' accountability, and to the credibility of Parliament itself'.'<sup>iii</sup>

Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014

#### 7.2 Recommendations

The offices of the Intelligence Services Commissioner and the Interception of Communications Commissioner should be reformed so that they are truly independent, reporting to Parliament not the Executive. They need adequate resources to scrutinise more warrants, carry out searching investigations and publish key statistics.

The ISC must be fully reformed if it is to provide meaningful parliamentary oversight. The committee should be answerable directly to Parliament rather than to the prime minister and take its own decisions on reporting and publication. The committee must be appropriately funded and staffed with independent experts able to undertake detailed forensic investigations, and an independent secretariat, including independent legal and technical advisors. The committee should have strengthened legal powers to compel the production of information and the attendance of witnesses. The chair of the committee should be a member

of the largest opposition party and the Commons members of the committee should be elected.

The Investigatory Powers Tribunal should adopt a more fair and open procedure. This should include: public hearings, unless the government demonstrates that secrecy is required in the particular case; evidence should be disclosed and judgments and reasons published unless the government demonstrates that secrecy is necessary; a special advocate should be appointed if a closed hearing is required; and decisions should be subject to appeal.

## 7.3 The Executive and Ministers

The UK has a number of bodies that oversee the surveillance activities of the security services, and in some cases, the police. One of the key threats to full democratic accountability is that these bodies are themselves accountable to the Executive and not to Parliament. Chairs and commissioners are appointed by the Prime Minister not our democratically elected MPs. This and other challenges to full democratic accountability are described below.

The executive also has primary responsibility for the agencies, as the ministers are ultimately responsible. In theory they provide a first line of accountability.

# 7.4 Interception of Communications Commissioner's Office

The IOCCO<sup>iv</sup> provides statutory independent oversight of the lawful interception of communications (under Part I Chapter I of RIPA), the acquisition and disclosure of communications data (under Part I Chapter II of RIPA) and the performance of the powers and duties conferred on the Secretary of State by Part III of RIPA (investigation of electronic data protected by encryption).

The current commissioner Rt Hon. Sir Anthony May, was appointed by the Prime Minister in January 2013.

The IOCCO has to date presented a yearly report<sup>v</sup> which normally contains long explanations of the law, but very little detailed information. In relation to interception warrants it simply gives an overall figure of authorisations – 2,760 in 2013, down from 3,371 in 2012, with some 1,669 active on the 31st December. In 2013 there were 514,608 requests for communications data. The report does not break these down into categories, such as the precise section of the law under which they were authorised or the type of investigation.

Following the Data Retention and Regulatory Powers Act 2014 (DRIPA) the IoCC now has to report twice a year.

#### 7.5 Intelligence Services Commissioner

The Intelligence Services Commissioner, currently the Rt Hon Sir Mark Waller, is appointed by the Prime Minister. He reviews the Secretary of State's issuing of warrants that authorise intrusive surveillance and interference with property under Part II of RIPA. He also reviews the use of directed surveillance and of covert human intelligence sources (i.e. agents) by the Intelligence Agencies, MOD and members of the armed forces to check that they are acting in accordance with the requirements of RIPA.

Although in principle the IOCCO has primary jurisdiction over interception, there is overlap with the IoCC (see section 7.2.1).

The Justice and Security Act 2013 has given additional functions to the ISC. He can be asked by the Prime Minister to review almost any functions of the intelligence and security services, as long as this does not interfere with the IoCC.

Importantly, he has oversight over any warrants issued under Sections 5 and 7 of the Intelligence Services Act (ISA, 1994).<sup>vi</sup> S5 warrants cover the interference with property or "wireless telegraphy", such as the installation of bugging devices. S7 warrants allow what would normally be unlawful conduct in the UK, as long as it takes place abroad. These could be very important in relation to the hacking activities of GCHQ.

The Intelligence Services Commissioner also monitors the agencies' compliance with the consolidated guidance for working with overseas partners in relation to detainees, which is meant to prevent collaboration in torture and other abuses.<sup>vii</sup>

The Intelligence Services Commissioner visits the agencies twice a year and examines a sample of warrants issued by the Secretaries of State authorising intrusive surveillance and interference with property. In 2013 he looked at 16.8% of the 1887 warrants issued under both RIPA and ISA. He ensures that the agencies apply the same authorisation process and the same test of necessity and proportionality. But his report does not explain how many warrants fall under each type of authorisation, so it is hard to scrutinise.

The Intelligence Services Commissioner was heavily criticised, including by the Home Affairs Committee, when he appeared to say that the extent of his investigation of the Snowden allegations had simply consisted in seeking verbal assurances from GCHQ leaders, and trusting the ethos of the agency. He has since stated that he had actually carried out a more thorough investigation and still believes that GCHQ's work is fully above board.<sup>viii</sup> In 2013 he examined 33 RIPA and ISA warrants from GCHQ.

## 7.6 Reforming the Commissioners

The offices of the Intelligence Services Commissioner and the Interception of Communications Commissioner should be reformed. Both are part time semi-retired judges (with few resources) appointed by the Prime Minister. Until the very recent inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources, the Commissioners have never publicly found a warrant to be disproportionate. In that inquiry the Interception Commissioner found that: police forces did not give the question of necessity, proportionality and collateral intrusion sufficient consideration; and the Home Office Code of Practice does not provide adequate safeguards to prevent unnecessary or disproportionate intrusions. He recommended that judicial authorisation is obtained in cases where communications data is sought to determine the source of journalistic information.<sup>ix</sup>

The commissioners should be truly independent, reporting to Parliament to be insulated from government influence.

In the absence of prior judicial authorisation for surveillance decisions, it is vital that all decisions be subject to ex post facto scrutiny by a judge. But the commissioners inspect only a small proportion of warrants. The IoCC checks around one third and the ISC around 17% of the warrants under their jurisdiction.

The Home Affairs Committee in parliament has made clear that the commissioners simply do not have the capacity to deal with the hundreds of thousands of surveillance requests in place every year. If the commissioners are to offer effective oversight, they must be empowered to conduct searching investigations, with adequate resources and the requirement to publish key statistics.

#### 7.7 Judicial Oversight and Ministerial Warrants

In the UK, the Secretary of State authorises interception warrants and senior officials authorise access to communications data. There is some qualified provision for judicial authorisation respect of intrusive surveillance by police (but not the intelligence services), requests for encryption keys, and for local authorities seeking access to communications data. There are also proposals to introduce judicial authorisation for the interception of the communications of journalists.

As we showed in Section 6.1.3, this arrangement allows the executive to self-authorise the use of surveillance powers, which is unacceptable. All intrusive, directed and targeted surveillance should be authorised by a serving judge. It is the function of the judiciary to act as a check on the executive.

English law has long recognised the need for a judicial warrant before a person's home can be searched by the police. There is no longer any meaningful distinction between the quantity and nature of personal information that can be collected during a premises search and that collected via the targeted surveillance practices permitted under RIPA.

#### 7.8 Intelligence and Security Committee

The Intelligence and Security Committee of Parliament (ISC) was created by the Intelligence Services Act in 1994<sup>x</sup> with a mandate "to examine the expenditure, administration and policy" of the secret and intelligence services.

The Justice and Security Act 2013<sup>xi</sup> introduced some reforms to the ISC, making it more independent from the executive and increasing its remit, including some oversight of operational activity and the wider intelligence and security activities of Government. But the reforms may not have huge practical implications.

A recent report<sup>xii</sup> by the Home Affairs Committee in the UK Parliament was hugely critical of the current oversight mechanisms of surveillance, particularly the ISC. The committee was found to be too cozy with the executive, despite recent changes to its statute.

The committee has an extremely tough job. It needs to be able to assess complicated technical questions, legal and human rights questions, and find means to assess the costs versus benefits of different approaches to secret investigations. None of the answers should be taken at face value from agencies. Thus experts in each field need to be consulted, not just through questions and evidence, but as part of the process of interrogating the secret services. This is similar for any scrutiny committee, but especially one with a particularly high level of responsibility.

There are several areas that will have been hard for the committee to fully analyse that are worth highlighting. For instance, the use of "zero day" exploits highlighted in Chapter Four comes with consequences, including the use of the same exploits by third parties such as criminals. Non-disclosure of exploits means that computer engineers who are trying to prevent their software from containing such exploits may be hindered in learning how and why certain rare or new kinds bugs have occurred. For the committee and GCHQ these are very tricky policy questions, that can only be properly answered through deep discussion with security engineers. The consequence of getting the policy wrong however is severe. It can result in insecure computing and financial or data losses from companies and individuals to automated criminality.

Another area we have touched on already is the problem of mass analytics, the power of computing and the question of intrusion. The committee has discussed this at some length in their hearings. They should however have examined the actual practices at GCHQ and the software capabilities directly, with the aid of computer scientists.

Although the committee can now vote its own chair, the members of the committee still have to be nominated by the Prime Minister. The most effective committees, such as the Public Accounts Committee, tend to have a chair from an opposition party. The Prime Minister also has to approve any investigation by the ISC. He has prior sight of the committee's reports to Parliament and may decide that matters should be excluded in the interests of national security. Secret agencies and government departments don't have an obligation to provide information for any investigation beyond the narrow oversight set out in 1994.

But even if given more powers, it is unclear whether the current committee has any appetite for deeper scrutiny. In July 2013, <sup>xiii</sup> soon after the first Snowden articles appeared, the ISC quickly cleared GCHQ of any wrongdoing about PRISM. According to one of its most prominent members, the Labour MP Hazel Blears, <sup>xiv</sup> the ISC was previously aware of GCHQ's mass surveillance practices, although not by the name TEMPORA, and were

satisfied that they were proportionate. But this has been called into question and a proper clarification in Parliament has not been provided.<sup>xv</sup>

As representative of the interests of citizens, the ISC has consistently failed in its duty to challenge the intelligence agencies, and reassure the rest of Parliament and the population. As the Joint Committee on Human Rights (JCHR) in Parliament has noted, the level of redaction of ISC reports is sometimes so great that 'it can be difficult to follow the Committee's work and to understand its reports.'

The ISC must be fully reformed if it is to provide meaningful parliamentary oversight. The committee should be answerable directly to Parliament rather than to the prime minister and take its own decisions on reporting and publication. The committee must be appropriately funded and staffed with independent experts able to undertake detailed forensic investigations and an independent secretariat, including independent legal and technical advice. The committee should have strengthened legal powers to require the production of information and to compel the attendance of witnesses. The chair of the committee should be a member of the largest opposition party and the Commons members of the committee should be elected.<sup>xvi</sup>

#### 7.9 The Investigatory Powers Tribunal

The Investigatory Powers Tribunal (IPT) is the sole body responsible for handling complaints and Human Rights Act claims from individuals about the interception of communications by public authorities under RIPA.<sup>xvii</sup> It deals with complaints about the conduct of the UK intelligence and security services, and even the police, for example in respect of the acquisition and disclosure of communications data.

The Tribunal can hear complaints on interception of communications and obtaining of communications data, intrusive surveillance, directed surveillance, interference with property, and investigation of protected electronic information. For example, the IPT has been dealing with some of the human rights complaints related to the scandals about undercover police officers in political and environmental movements.

The IPT is not a true court as the term is commonly understood. It operates with utmost secrecy and only has around three public hearings a year. In March 2014 it was revealed that the IPT had operated from the Home Office building for the past 14 years. In addition one of its staff members previously worked for the Office of Security and Counterterrorism, the heart of secret operations at the Home Office. These revelations raise serious questions about its independence.<sup>xviii</sup>

Before the IPT's judgment in the claim brought by Liberty, Privacy International and Amnesty International in February 2015,<sup>xix</sup> it had upheld only 10 out of over 1,500 complaints presented by members of the public.

#### 7.10 Individuals and Redress

Individuals are not usually notified that they have been subject to surveillance, which makes it very difficult to seek a remedy for violations of the right to privacy. We believe individuals should be notified after the event, unless there is a specific reason for not notifying a particular individual.

The IPT has the power to award compensation, make an order quashing or cancelling a warrant or authorisation, or make an order requiring the destruction of any records of information obtained via a warrant or authorisation or held by a public authority.<sup>xx</sup> However, as discussed above, the IPT has found in favour of claimants in only a tiny proportion of cases.

Where the IPT finds against a complainant it does not give reasons for its decision. As a result, the individual will not know whether that means the activity complained about occurred but was authorised and conducted lawfully, or that it did not occur at all. This is unsatisfactory. Importantly, there is no right of appeal against decisions of the IPT. Claimants who are unsuccessful in the IPT may have recourse to the European Court of Human Rights, but are unable to obtain a domestic remedy. In our view there should be a right of appeal to ensure individuals are able to enforce their rights.

The IPT's procedure is also unfair and disadvantages claimants. The IPT is not obliged to hold oral hearings and even where it does, these may be 'closed' secret hearings. There is no special advocate to represent the claimant at closed hearings. There should be a presumption that hearings will be held in open court unless there is a compelling case otherwise.<sup>xxi</sup>

We need a more effective system of redress so that individuals are able to obtain a remedy for violations of their rights. Accountability means that individuals should be notified that they have been subject to surveillance after the event, unless there is a specific reason for maintaining secrecy. Otherwise, as discussed above, it is almost impossible to obtain an effective remedy.

The US has seen a more mature debate on this issue. The President's Review Group on Intelligence and Communications Technologies argued for increased transparency and called for legislation that permits telecommunications companies to disclose information about the orders they receive from the government.<sup>xxii</sup> They also recommended 'civilian' involvement in the oversight of surveillance, alongside greater involvement for public interest advocates.

## 7.11 Admissibility of Intercepted Communications

At present material gathered from intercepted communications, known as intercept evidence, is inadmissible in legal proceedings under section 17(1) of RIPA. In other countries the same restriction does not apply. Intercept evidence should now be made admissible in criminal proceedings. This is a change that is supported by former Directors of Public Prosecutions, but opposed by GCHQ as it would disclose to the public the scale of interception activity. However, keeping the evidence out of the courts has the effect of making accountability for surveillance activities very hard indeed.

From a human rights perspective there is nothing to prevent the use of intercept material, properly authorised by judicial warrant, in criminal proceedings. In fact, allowing evidence gained through intercept to be used in criminal trials would enable greater judicial oversight. The European Court of Human Rights has found that the potential to exclude illegally obtained surveillance was an important safeguard that discouraged the collection of evidence by unlawful means.<sup>xxiii</sup> Making intercept admissible would also increase the number of possible prosecutions of serious criminal and terrorists and therefore should discourage the government from resorting to other means such as control orders.

#### **Reviews of Surveillance Practices**

There are three ongoing reviews of the government's surveillance practices. The Independent Reviewer of Terrorism Legislation, David Anderson QC, is completing an 'Investigatory Powers Review' as mandated by the Data Retention and Investigatory Powers Act (DRIPA). This will consider the capabilities and powers required by law enforcement and the security intelligence agencies and the regulatory framework within which those capabilities and powers should be exercised.<sup>xxiv</sup> DRIPA provides that the Independent Reviewer must, so far as reasonably practicable, complete the review before 1 May 2015.<sup>xxv</sup>

The Royal United Services Institute (RUSI) has been tasked by the Deputy Prime Minister, Nick Clegg, to conduct an independent review. This will cover surveillance technologies and the problems of control and oversight in the context of new communications technologies. The panel of 12 experts will make recommendations for legislative and policy reform and will report after the general election.<sup>xxvi</sup>

Parliament's Intelligence and Security Committee is conducting its own Privacy and Security Inquiry. This will consider whether the current statutory framework governing access to private communications remains adequate and the appropriate balance between our individual right to privacy and our collective right to security.<sup>xxvii</sup> We expect it to release its report imminently.

It is notable that in the UK there has been no comprehensive parliamentary inquiry similar to the one taking place in Germany, where the Bundestag has specifically established a cross party committee of inquiry for the purpose and tasked it with answering specific and probing questions.<sup>xxviii</sup>

#### 7.12 Conclusion

Citizens must be sufficiently informed about the scope and nature of surveillance operations to be able to hold government to account. Increased transparency on the scale and reach of surveillance does not need to threaten operational secrecy.

The reports from the independent commissioners only give overall figures of numbers of interceptions, authorisations and warrants, including some errors and mistakes. But this is not enough to understand the true picture of state surveillance. Some warrants will refer to a single individual while others could authorise wholesale surveillance or hacking affecting

thousands of people. While the work of the ICC in particular seems to be improving, the commissioner system needs revisiting and is not a replacement for judicial oversight.

The lack of an independent Parliamentary committee is well-known. The reaction of the ISC during the last two years has not built confidence, from its apparent ignorance of the programs, to its steadfast backing of the agencies. Yet its job is crucial. It seems highly likely that it should have been able to spot the change from targeted interception to bulk collection, and the need for Parliamentary approval through new legislation, yet it did not. Combined with the lack of judicial authorisation for bulk collection warrants, the UK's system of accountability has been shown to lack effective restraint. The result is challenges in the European courts (see section X).

There has been a historic refusal to contemplate transparency on the methods and capabilities of the services, with the argument that this would give away critical information to our enemies. But the widespread surprise and shock generated by the Snowden leaks demonstrates the need for a public debate on the scale and overall capacities of surveillance programmes.

Sometimes supporters of the status quo will point to opinion polls that show that the public is broadly supportive of the agencies. Other polls of course point to disquiet and an appetite for a full discussion of the issues, perhaps showing that the policies are not fully understood. But the genuine question of accountability cannot be answered through a public opinion test: significant sections of the public are increasingly distrusting of state surveillance, which is a corrosive situation for the agencies themselves.

This distrust and unease extends in different ways to some lawyers, journalists, campaigners, human rights bodies and minority communities who may feel wrongly targeted. Many of the groups where distrust will build most are those who security agencies most need confidence from.

We should also note that most oversight mechanisms do not automatically lead to a significant curtailing of the activities of any of the agencies. In fact, oversight should be the easy part. If we are in trouble agreeing even these reforms, then we are in significant danger of permanently losing control of our agencies and putting trust in our agencies on a long term path of decline.

#### GCHQ and UK Mass Surveillance

i http://www.theguardian.com/commentisfree/2013/oct/20/parliament-forsaken-liberty-law-last-resort ii https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/335208/Surveillance\_road\_map\_ v3 1.pdf

iii 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

iv http://www.iocco-uk.info/default.asp

v http://www.iocco-

uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf vi http://www.legislation.gov.uk/ukpga/1994/13/section/5

vii

 $https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62632/Consolidated_Guidance_November_2011.pdf$ 

viii

http://isc.intelligencecommissioners.com/docs/40707\_HC304IntelligenceServicesCommissioner\_Accessible.pdf ix http://www.iocco-uk.info/docs/Press%20Release%20IOCCO%20Journalist%20Inquiry.pdf, http://www.iocco-

uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf x http://www.legislation.gov.uk/ukpga/1994/13/section/10

xi http://www.legislation.gov.uk/ukpga/2013/18/part/1/crossheading/oversight-by-the-intelligence-and-security-committee-of-parliament/enacted

xii http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23108.htm

xiii http://www.statewatch.org/news/2013/jul/uk-isc-gchq-surveillance-statement.pdf

xiv http://www.independent.co.uk/news/uk/home-news/hazel-blears-says-security-committee-did-know-the-scope-of-gchq-snooping-8928888.html

xv http://www.theyworkforyou.com/lords/?id=2013-11-20a.957.0

xvi Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 158,

available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

xvii under Part IV of RIPA

 $xviii \qquad http://www.theguardian.com/politics/2014/mar/05/independence-ipt-court-mi5-mi6-home-office-secrecy-clegg-miliband$ 

xix Liberty and Others, IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH

http://www.ipt-uk.com/docs/Liberty\_Ors\_Judgment\_6Feb15.pdf

xx Section 67(7) Regulation of Investigatory Powers Act,

http://www.legislation.gov.uk/ukpga/2000/23/section/67

xxi The Supreme Court concluded similarly in *Bank Mellat (Appellant) v Her Majesty's Treasury (Respondent) (No. 1)* [2013] UKSC 38, https://www.supremecourt.uk/decided-

cases/docs/UKSC 2011 0040 PressSummary.pdf

xxii http://www.whitehouse.gov/sites/default/files/docs/2013-12-12\_rg\_final\_report.pdf

xxiii Uzun v. Germany (application no. 35623/05)

xxiv https://terrorismlegislationreviewer.independent.gov.uk/review-of-communications-data-and-interception-powers/

xxv Data Retention and Investigatory Powers Act 2014, section 7

http://www.legislation.gov.uk/ukpga/2014/27/section/7/enacted

xxvi

https://www.rusi.org/go.php?structureID=S430F4009EEE86&ref=N5315B2C9B1941#.VNDOQik\_NlJ xxvii https://b1cba9b3-a-5e6631fd-s-

sites.googlegroups.com/a/independent.gov.uk/isc/files/20131211\_ISC\_Call\_for\_papers-

 $\label{eq:privacy.pdf} Privacy.pdf? attachauth=ANoY7 co3Zg_2avMuT4 aayl8NbU8Oi5VS1 a7XdKrdA3IgomOd21Uew3l8oSYi4vRAdrqO0hUUiQ9F-$ 

TdUQbjkN2eV0iA4euQA3RrqUOryF6EHsrvt6Mx80C6mCU74Rrl3MI5IldfxTA4q4IAGUKNPYJt3gByZpJpg

 $ITJmzbdmktIvGj0GcEt-MGrkU312CDFhDozvHxbPtV59iPeJoRQnDwmpvi2PDefE-P_28-L1tx8LL6d92RFTY-NjtdOHy4a1x73Zr7p7IaEf&attredirects=0xxviii$ 

 $https://www.bundestag.de/blob/284528/a89d6006f28900c4f46e56f5e0807ddf/einsetzungsantrag\_englisch-docx-data.pdf$