Intelligence and Security Committee

Annual Report 2010–2011

Chairman:
The Rt. Hon. Sir Malcolm Rifkind, MP

Intelligence and Security Committee

Annual Report 2010–2011

Chairman:

The Rt. Hon. Sir Malcolm Rifkind, MP

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
by Command of Her Majesty
July 2011

Cm 8114 £20.50

Any enquiries regarding this publication should be sent to us at committee@isc.x.gsi.gov.uk

This publication is available for download at www.official-documents.gov.uk.

This document is also available from our website at http://isc.independent.gov.uk

ISBN: 9780101811422

Printed in the UK for The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office

ID 2441486 07/11

Printed on paper containing 75% recycled fibre content minimum.

From: The Chairman, The Rt. Hon. Sir Malcolm Rifkind, MP

INTELLIGENCE AND SECURITY COMMITTEE
35 Great Smith Street, London SW1P 3BQ

ISC 2010/11/160 7 July 2011

The Rt. Hon. David Cameron, MP
Prime Minister
10 Downing Street
London
SW1A 2AA

Dear Prime Minister,

I enclose the Intelligence and Security Committee's Annual Report for 2010–2011. This Report details the work and conclusions of the Intelligence and Security Committee for the period from October 2010 to May 2011. The Committee has held 19 formal sessions during this period.

The majority of the Committee's time during the reporting period was spent examining and taking evidence on the work of the three intelligence and security Agencies and the wider intelligence community. We report on these matters here.

In addition to this Report, the Committee has submitted proposals separately to the Government on how oversight of the Agencies could be strengthened – in particular through reform of this Committee – in the context of the forthcoming Green Paper on handling of intelligence in judicial proceedings.

Yours sincerely

MALCOLM RIFKIND

THE INTELLIGENCE AND SECURITY COMMITTEE

The Intelligence and Security Committee (ISC) is an independent Committee established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the three UK intelligence and security Agencies: the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee also examines the work of the Joint Intelligence Organisation and the National Security Secretariat in the Cabinet Office, Defence Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism in the Home Office.

The Prime Minister appoints the ISC Members after considering nominations from Parliament and consulting with the Opposition. The Committee reports directly to the Prime Minister and through him to Parliament, by the publication of the Committee's reports. The Prime Minister may ask us to look into a matter, but most of the time we set our own agenda.

The Committee has an independent Secretariat currently hosted by the Cabinet Office. The Committee also has access to a General Investigator to undertake specific investigations covering the administration and policy of the Agencies; a Financial Investigator covering expenditure issues; and a Legal Advisor to provide independent legal advice.

The Members of the Committee are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are given access to highly classified material in carrying out their duties. The Committee holds evidence sessions with Government Ministers and senior officials (for example, the Head of the Security Service). It also considers written evidence from the intelligence and security Agencies and relevant government departments. This evidence may be drawn from operational records, source reporting and other sensitive intelligence, or it may be memoranda specifically written for the Committee.

The Prime Minister publishes the Committee's reports: the public versions have sensitive material that would damage national security blanked out ('redacted'). This is indicated by *** in the text. The intelligence and security Agencies may request the redaction of sensitive material in the Report which would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee considers these requests for redaction in considerable detail. The Agencies have to demonstrate clearly how publication of the material in question would be damaging before the Committee agrees to redact it. The Committee aims to ensure that only the bare minimum of text is redacted from the Report. We also believe that it is important that Parliament and the public should be able to see where we have had to redact information, rather than keeping this secret. This means that the Report that is published is the same as the one sent to the Prime Minister: there is no 'secret' report. Under the existing legislation the Prime Minister has the power to redact material without the Committee's consent, making a statement to that effect when he lays the Report before Parliament. To date, this has never happened.

CONTENTS

SECTION 1: THE WORK OF THE COMMITTEE

1. This Report details the work and conclusions of the Intelligence and Security Committee (ISC) for the period from October 2010 to May 2011.[1] The Committee has held 19 formal sessions during this period.

2. The majority of the Committee's time during the reporting period was spent examining and taking evidence on the work of the three intelligence and security Agencies and the wider intelligence community. We report on these matters here.

3. The ISC was established under the Intelligence Services Act 1994 and has now been operating for over 16 years. We consider that it is right to review whether the structure, remit and powers of the Committee are still sufficient in the context of the current intelligence machinery. We have therefore conducted a root-and-branch review, taking the 1994 legislation as a starting point, but also recognising that the work of the Committee has evolved considerably since. We have also taken into account the forthcoming Green Paper on the handling of intelligence material in judicial proceedings. We have provided proposals to the Prime Minister as to how this Committee can be strengthened and, in particular, how to provide greater openness and transparency, and reassurance to the public and Parliament. Our recommendations are covered further in paragraphs 270 to 274.

4. In addition to its formal evidence sessions with the three Agencies, the Committee has also taken evidence from Defence Intelligence, the Joint Intelligence Committee (JIC) and the National Security Adviser, as well as the Foreign Secretary and the Home Secretary. The Committee has visited all three intelligence and security Agencies and Defence Intelligence in the Ministry of Defence. We have held bilateral discussions with key officials in the US and Canadian intelligence communities, and hosted parliamentarians and officials from Canada, Kenya and Mexico. The Chairman has also contributed to a number of intelligence-related seminars and conferences in the UK.

[1] *The current Committee was formally constituted in October 2010; however, we have taken evidence covering the period from April 2010.*

SECTION 2: KEY THEMES

5. Intelligence remains of critical importance in contributing to the first duty of government: keeping its citizens safe. The UK intelligence machinery has a justifiably proud history and strong reputation among its partners around the world. The Committee has been impressed by the dedication, professionalism and commitment of those members of the intelligence community it has met.

6. There are a number of key themes and conclusions which have emerged from our work this year which are summarised briefly below. While some of these highlight problems or concerns, they should not detract from our view that those working in this field continue to excel at a tremendously challenging task.

2010 Spending Review

7. Given the scale of cuts across the rest of the public sector, the intelligence and security Agencies received a fair settlement as part of the 2010 Spending Review. Nevertheless, it presents them with a significant challenge: after a decade of growth, they now face 'flat-cash' funding for the next four years. Taking account of inflation, this represents a real-terms cut of at least 11%. This will inevitably have an impact on the ability of all three Agencies to maintain current levels of coverage of the threat. It is essential – given the fundamental importance to our national security of the Agencies' work – that the settlement is kept under review and that there is scope to adjust it if there is a significant change in the threat. (Paragraphs 41 to 46.)

8. The Olympics are of particular concern, both in terms of the increased threat to the UK during the Games, and the resources available to tackle it. The Director General of the Security Service has stated publicly that the 2012 Olympics will represent a significant target for terrorist groups, saying that "*the eyes of the world will be on London during the Olympics… [and] those eyes will include some malign ones that will see an opportunity to gain notoriety and to inflict damage*". The Security Service has told us that it has planned for this increased threat, including through the recruitment of additional intelligence officers. The Director General has also told us that he considers the Service to be well placed to manage the risks that the Olympics will bring. However, we have also been told that the effort required to cover the Olympics will inevitably divert resources from the Service's other work. This is a matter of very serious concern. If the Security Service cannot be resourced to cover the additional work that the Olympics will bring, then the National Security Council (NSC) must take such steps as are necessary to minimise the risk. (Paragraphs 93 to 95.)

The National Security Council and central intelligence machinery

9. This Committee has repeatedly highlighted the need for a more effective Ministerial forum for national security matters and we therefore welcome the establishment, in May last year, of the National Security Council. Witnesses have described it as a significant improvement on the previous system: one of the key benefits is the opportunity it provides for more regular contact between the Heads of the intelligence and security Agencies and Ministers. The NSC must maintain its current status and priority. (Paragraphs 125 to 129.)

10. The establishment of a new body such as the NSC inevitably necessitates a restructuring of the existing mechanisms underneath it. It has become very clear to the Committee that, whilst the NSC's setting of priorities through the National Security Strategy is welcome, there is now a need to align the other mechanisms through which the Agencies are tasked. In addition to the National Security Strategy, the Agencies also currently take direction from the national security tasks outlined in the Strategic Defence and Security Review (SDSR), the JIC Requirement and Priorities (R&P) process, and also their own existing Agency Strategic Objectives and Treasury targets. This could potentially lead to confusion and conflict. We therefore welcome the current review of central intelligence and security structures and expect this to establish a clear, simplified tasking process flowing from the National Security Council, supported by a more clearly aligned JIC R&P process. (Paragraphs 139 to 142.)

Cyber security

11. In its 2008–2009 Annual Report, the ISC raised concerns about the potential threat posed to the UK Government, Critical National Infrastructure and commercial companies from electronic attack and recommended that the UK accord cyber security a higher priority. We therefore welcome the fact that this threat has been recognised and that cyber security is now listed as a Tier One national security risk. The new funding that has been made available, as part of the SDSR, to fund cyber security work is a significant step forward.

12. Whilst the priority and funding are to be welcomed, structural issues continue to cause us concern. We have noted 18 units with particular responsibilities in this field across the three Agencies, two law enforcement bodies and five government departments. Between them they cover policy, management, intelligence operations, protective advice, detection and analysis, with some focused on crime, some on hostile activity from overseas, some on Counter-Terrorism and others covering all three. This risks duplication and confusion and cannot be cost-effective. We therefore recommend that work be done to rationalise the existing structures.

13. Of perhaps even greater concern, however, were the arrangements for central co-ordination and Ministerial responsibility. It was neither sensible nor appropriate to assign Ministerial responsibility for cyber security to the Home Office when officials were themselves split between the Cabinet Office and GCHQ. This was fundamentally flawed, as has been acknowledged in evidence to us. Decisions relating to national security demand the clearest lines of Ministerial accountability. We therefore welcomed the Government's decision to simplify this structure by transferring responsibility for cyber security to the Minister of State in the Cabinet Office. (Paragraphs 186 to 195.)

Detainees

14. On 6 July 2010, the Prime Minister announced a package of measures which aimed to draw a line under allegations made by former detainees that the UK Agencies may have been complicit in their mistreatment by some of our allies. The first step was the publication of the Consolidated Guidance for intelligence officers and Armed Forces

personnel on dealing with detainees overseas. We welcome the publication as a move towards greater transparency and openness. The ISC in the last Parliament provided a valuable contribution to the formulation and improvement of this policy, reporting to the then Prime Minister on the legal and policy framework within which the Agencies and Armed Forces must operate, and recommending a number of changes to the guidance including that there should be greater clarity around Ministerial involvement and decision-making. Whilst the finalised guidance – which incorporated some of the Committee's recommendations – was published in July 2010, the Prime Minister decided not to publish the previous Committee's report since it related to the draft guidance rather than the final, published version.

15. One of the other measures in the package was the settlement of the civil claims against the Government by former detainees. In November 2010, an agreement was reached with the former Guantánamo Bay detainees which admitted no liability on the Government's part, and which resulted in the civil claims against the Government being withdrawn. The payment of public money to former Guantánamo Bay detainees will have been unpalatable to many people, but having considered the confidential terms of the settlement, and the likely impact on our national security of liaison material being released during the court process, we have concluded that it was overwhelmingly in the public interest that a settlement was reached. (Paragraphs 210 to 217.)

16. Court cases have raised serious concerns regarding the treatment of classified intelligence material in judicial proceedings. It is a matter of grave concern that, in the Binyam Mohamed case, the Court of Appeal's decision resulted in the release of US intelligence material. While that material was not highly sensitive in itself, we heard first hand from US authorities their concerns about the actions of the UK courts and the strain this has put on the UK's security partnership with the US. It is essential that this matter be resolved urgently, and we therefore welcome plans to publish a Green Paper on the protection of sensitive material in court proceedings later this year. (Paragraphs 226 to 231.)

7/7 Inquests

17. The Inquests into those who died in the terrorist attacks on 7 July 2005 concluded in May 2011. One of the issues considered by the Coroner was that of 'preventability' and the Committee therefore provided the Coroner with access to the Committee's own investigations on this issue. The Coroner's conclusion that the police and the Security Service could not reasonably have prevented the 7/7 bombings given the resources at their disposal and the high priority threats they were facing mirrors the Committee's own conclusions in its 2009 Report.

18. The Coroner did criticise the Service's procedures for showing photographs to sources, and for recording its decisions relating to the assessment of targets. We share those concerns and will be monitoring the Security Service's response to these recommendations. (Paragraphs 232 to 237.)

19. The Coroner acknowledged the ISC's second report on the 7 July 2005 terrorist attacks as being "*detailed and thorough*". However, during the course of the Inquests a small number of discrepancies between evidence provided by the Security Service to this Committee and that provided to the Coroner came to light. Some of these were very minor inaccuracies relating to points of detail such as dates or addresses. However, three were of substance (these are covered in detail in paragraph 240). The Coroner therefore suggested that consideration should be given "*to whether procedures can be improved to ensure the accuracy and completeness of information provided by the Security Service to the ISC*".

20. We have satisfied ourselves that these inaccuracies would not have altered our findings or recommendations, had we known about them. Nevertheless, it is extremely frustrating, both for the Committee and for those who rely on our reports, that these errors were not detected when draft versions of our reports were shared – over the course of a year – with the Security Service (and others) for them to check the facts for accuracy. This Committee has repeatedly, since 2007, drawn attention to the poor state of the Agencies' records. In May 2009, in a letter to the then Prime Minister, we warned that:

> *The Agencies must conduct thorough research in support of any information provided to the Committee. When information emerges after the Committee has reported on a matter, it damages trust in this Committee, undermines our credibility and harms democratic accountability… If all branches of Government cannot keep this Committee properly informed, oversight of the Agencies will inevitably be played out through the courts.*

We must now see significant improvements in this area. (Paragraphs 238 to 244.)

The Committee's Investigator

21. Last year, our Investigator undertook an assessment of national security vetting in the Agencies. Based on that investigation, and subsequent evidence from the Agencies, we accept the continued requirement for the Agencies to conduct vetting separately from other parts of Government. However, the rationale for each Agency to maintain its own separate vetting system is less compelling, particularly when there are potentially cost savings to be made. We therefore recommend that consideration is given to a single vetting unit for the Agencies. (Paragraphs 266 to 269.) Our Investigator has since begun an assessment, with the National Audit Office, of the considerable capital projects within GCHQ's signals intelligence modernisation programme (SIGMOD) and is expected to report shortly.

Reform of the Intelligence and Security Committee

22. In the 16 years since the ISC was established there have been a number of changes within the intelligence community, and the work of the Committee has evolved to take account of these. However, public expectation in terms of transparency and openness has increased significantly during this time, and it is essential that the Committee's status, remit and powers enable it to provide credible reassurance to the public and to Parliament.

Therefore, since the Committee was constituted last year, we have undertaken a root-and-branch review of the Committee. We have concluded that the current arrangements are significantly out of date and it is time for radical change. The *status quo* is unsustainable.

23. The Government's Green Paper on the protection of intelligence material in the courts provides not only an excellent opportunity for change, but also the impetus: if there are to be changes in the powers of the courts then this must be counter-balanced by strengthened independent oversight of the Agencies. We have produced proposals for change, designed to increase accountability, transparency and capacity for oversight of the intelligence community. In particular, we are recommending that the ISC should become a Committee of Parliament with the necessary safeguards. We believe these recommendations should form the basis for the relevant sections of the forthcoming Green Paper. (Paragraphs 270 to 274).

SECTION 3: THE NATURE OF THE THREAT

24. The threat to the United Kingdom and its interests overseas comes from a number of sources including international and Northern Ireland-related terrorism, Hostile Foreign Activity and nuclear proliferation. The three intelligence and security Agencies work with the wider intelligence community to counter these threats.

International terrorism

25. Since 22 January 2010, the Joint Terrorism Analysis Centre (JTAC) has assessed the threat to the UK from international terrorism as "SEVERE".[2] This means that the threat of a terrorist attack is considered to be highly likely.

26. The primary threat comes from Al-Qaeda. The National Security Strategy, published in October 2010, described the Al-Qaeda threat in the following terms:

> *Al-Qaeda wants to use violence to overthrow governments in the Middle East to create a caliphate, a unified government for the Muslim world based on an extreme interpretation of Islam. By launching terrorist attacks against the US and its allies, Al-Qaeda hopes to remove western influence from the Islamic world.*[3]

27. Al-Qaeda Core[4] in the tribal areas of Pakistan and Afghanistan continues to pose the most serious strategic threat to the UK, and the Security Service assesses that this is likely to remain the case for the foreseeable future. However, the threat has diversified: the percentage of priority plots and leads that the Security Service investigates in the UK which are linked to Al-Qaeda Core has dropped from around 75% in 2008/09 to around 50% now.[5]

28. The death of Usama bin Laden, the leader of Al-Qaeda, on 1 May 2011 was described by the Security Service as being "*a key milestone in the defeat of Al-Qaeda*". The Service assesses bin Laden's death to have had the following impact:

> *The most important blow caused by the death of Usama bin Laden is to the morale and cohesion of Al-Qaeda Core, its affiliate groups and the global jihad more generally. For the majority, [he] was the inspirational figurehead and served to unite different nationalities, tribes and, to some degree, causes.*[6]

29. Nevertheless, it assesses that:

> *[Al-Qaeda's] operational activity will continue to pose a direct threat to the West despite the death of its leader: individuals may be encouraged or inspired to avenge Usama bin Laden's death… and Al-Qaeda Core's operational arm will continue to plot international attacks in the longer term.*[7]

---

[2] *www.mi5.gov.uk/output/threat-levels.html. Threat level at the time of writing.*

[3] *Cm 7953.*

[4] *Al-Qaeda Core refers to the few hundred operatives in the Federally-Administered Tribal Areas (FATA) of Pakistan and, occasionally, in Afghanistan, including the group's senior leadership.*

[5] *Briefing provided by the Security Service, April 2011.*

[6] *Briefing provided by the Security Service, May 2011.*

[7] *Ibid.*

30. There are now a number of affiliated groups in Somalia, Yemen and Iraq that share Al-Qaeda's name, broad objectives and methods. Al-Qaeda Core's Yemen affiliate, Al-Qaeda in the Arabian Peninsula (AQAP), was responsible for two narrowly averted attacks against Western aviation targets during 2009/10 (the Christmas Day 2009 underwear bomb targeting Detroit and the two printer cartridge bombs detected at East Midlands and Dubai airports in October 2010). The involvement of Yemen-based preacher Anwar Al Awlaqi in AQAP is of particular concern to the intelligence and security Agencies as he has a wide circle of followers in the West, including the UK, largely due to his use of English-language internet broadcasts. This was illustrated by the conviction of Rajib Karim[8] in February this year for a number of terrorist offences.[9] The Security Service assesses that any short-term attacks against Western targets in retaliation for the death of Usama bin Laden are more likely to be carried out by AQAP than Al-Qaeda Core.

31. The work of AQAP and Al Awlaqi to encourage extremists through online material has widened the potential threat to encompass individuals who are inspired (but not trained or directed by Al-Qaeda) to mount independent attacks.[10]

Northern Ireland-related terrorism

32. There continues to be a threat of terrorism in Northern Ireland, principally from republican terrorist groups.[11] The Northern Ireland-related threat levels published on 24 September 2010 judged the threat to Northern Ireland itself to be "SEVERE" and highlighted that the threat to the rest of the UK had been raised to "SUBSTANTIAL".[12]

33. The threat is not on the same scale as that from the Provisional IRA at the height of the Troubles. The Security Service has told the Committee that the numbers of individuals involved with the current republican terrorist groups is around half the number that were active in the Provisional IRA, and that the groups lack a coherent political agenda and have little popular support.[13] The threat, however, remains serious, and the number of attacks in Northern Ireland is increasing. In 2010 there were 40 attacks on national security targets, up from 22 in 2009, which is an increase of approximately 80%.[14]

34. The vast majority of republican terrorist activity is directed at the security forces, principally the Police Service of Northern Ireland, as was shown by the murder of Constable Ronan Kerr in April this year and other, unsuccessful, attacks targeting the police. However, there have also been attacks against targets other than the security forces. The discovery of a 500lb bomb near Newry on 7 April is a worrying indication of the increasing strength and activity of these dissident groups.

---

[8] *Karim, a British Airways employee, was jailed for 30 years for planning terrorist offences using his position in the company to enable an attack on transatlantic aviation. Karim was in contact with Al Awlaqi using sophisticated covert communication techniques, and conspired with Al Awlaqi and others to commit terrorist attacks, particularly against US-bound flights from the UK.*

[9] *Briefing provided by the Security Service, April 2011.*

[10] *Ibid.*

[11] *The Security Service assesses the current threat from the main loyalist groups as "LOW" (i.e. an attack is unlikely), although it acknowledges that there is a likelihood that small loyalist splinter groups will continue to engage in intermittent sectarian attacks.*

[12] *www.homeoffice.gov.uk/media-centre/news/terrorist-threat*

[13] *Oral Evidence – Security Service, 9 February 2011.*

[14] *Briefing provided by the Security Service, April 2011.*

Cyber security

35. Businesses and individuals increasingly use, and depend on, the internet. This brings with it security risks. The UK faces a constant threat of cyber attack from criminals, other states and, potentially, terrorists. This was recognised in the Government's National Security Strategy, which graded hostile attacks on UK cyber space a Tier One (i.e. highest) risk. Although most of the threat is currently from criminals seeking to defraud individuals and businesses, the internet also provides new opportunities for states – in particular, China and Russia – to conduct espionage against the UK.

Hostile Foreign Activity

36. The threat to British interests from espionage remains high. The commercial sector as well as government, defence and security interests are at risk from traditional espionage and (as a result of the revolution in global communications) through cyber space. Several major countries are actively targeting UK information and material to enhance their own military, technological, political and economic programmes.

Nuclear proliferation

37. The UK is also engaged in international efforts to prevent nuclear proliferation in the Middle East, with a particular focus on Iran. The intelligence community judges that, if Iran acquires nuclear weapons technology, there is a strong possibility that other states in the region will follow. The National Security Strategy says:

> *A Middle East with several nuclear weapons states would lead to high instability, precarious energy security and would have a severely damaging effect on the Middle East Peace Process.*[15]

[15] *Cm 7953.*

SECTION 4: THE AGENCIES

The Single Intelligence Account

38. The Single Intelligence Account (SIA) is the total budget voted by Parliament for the three intelligence and security Agencies. Following the terrorist attacks in the US on 11 September 2001, and the recognition of an increased threat to the UK from Al-Qaeda, the UK Government began to increase funding to the Agencies. After the terrorist attacks in London on 7 July 2005, the Government accelerated the planned funding increases. As a result the SIA has increased from approximately £800m to £2bn (in cash terms) over the last decade.

39. Over the last Comprehensive Spending Review (CSR07) period, the combined resource and capital budgets for the Agencies increased by 16.5% in cash terms:

	2007/08	2008/09	2009/10	2010/11
SIA (£m)[16]	1,648	1,815	1,914	1,920

40. In December 2009, the ISC in the last Parliament noted that, given the economic climate, the outlook for the SIA settlement in the next Spending Review was likely to be very different to the significant growth that had been experienced up to this point.[17] The previous ISC recommended that future funding settlements must nevertheless allow the Agencies to consolidate the gains of recent years in terms of resources and capabilities.

2010 Spending Review

41. In October 2010, the Government announced the results of its Spending Review for the four-year period beginning April 2011 (SR10). This provided a near 'flat-cash' settlement for the SIA.

	2011/12	2012/13	2013/14	2014/15
SIA (£m)[18]	1,996	1,984	1,990	1,965

42. In addition to the Agencies' core funding, an extra £600m will be made available over the Spending Review period for work related to cyber security.[19] Current planning has approximately half of this new funding going to the intelligence and security Agencies; in addition, GCHQ will also reallocate £50m of its SIA funding to cyber work.

---

[16] *Resource Departmental Expenditure Limit (DEL) plus Capital DEL on a full resource budgeting basis, net of depreciation. Figures taken from Spring Supplementary Estimates in the relevant year, reflecting actual budgets voted by Parliament, rather than budgets as set out when CSR07 was originally published.*

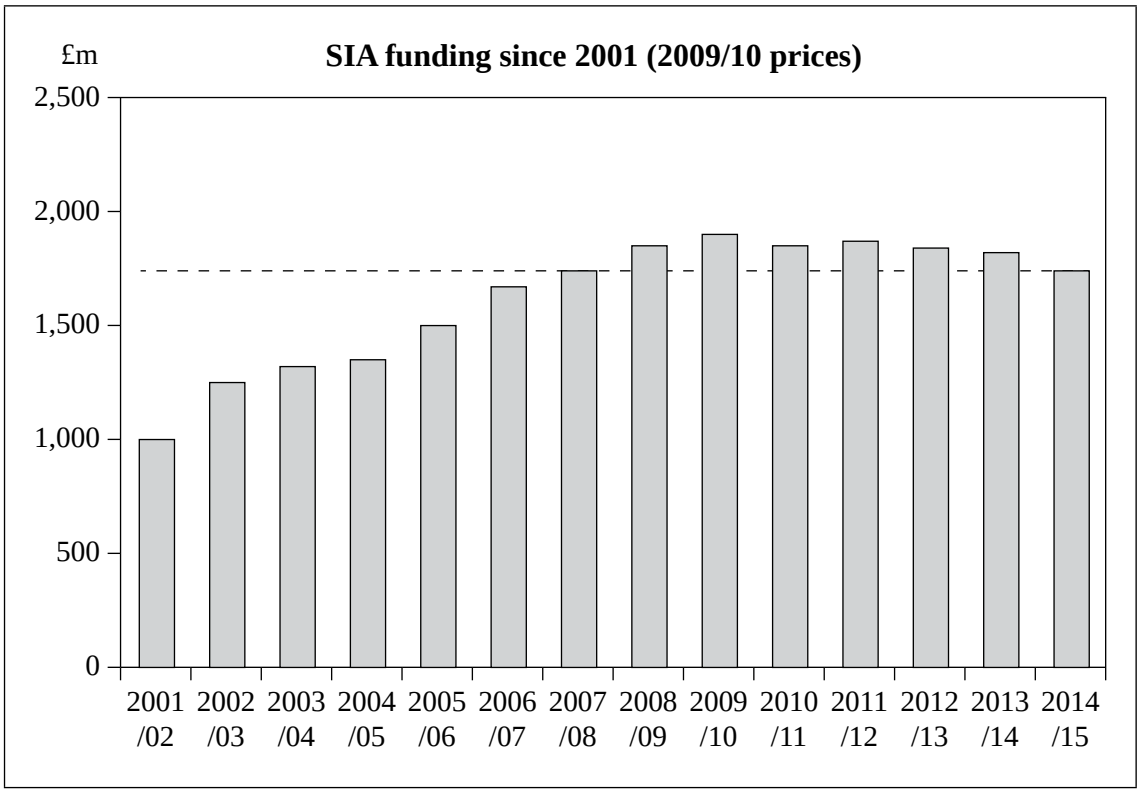
[17] *Cm 7807.*

[18] *Core SIA settlement – 'near-cash' (Resource DEL plus Capital DEL, excluding depreciation, Annually Managed Expenditure, and ring-fenced funding for cyber security). This includes £50m of cyber funding over the SR10 period contributed by the SIA and ring-fenced funding in years 3 and 4 of SR10 for Counter-Terrorism work.*

[19] *Cyber security is covered in more detail at paragraphs 186 to 207.*

The Security Service will also receive extra funding – up to £***m per year – following the Government's review of Counter-Terrorism powers, which will see Control Orders replaced by Terrorism Prevention and Investigation Measures (TPIMs).[20] These additional funding streams have not yet been allocated beyond 2011/12, and therefore total funding figures for the Agencies over the entire SR10 period cannot be provided.

43. Over the course of the four-year SR10 period this represents a real-terms cut of approximately 11.3% in the SIA. However, the actual impact is likely to be more severe since the rate of inflation has – at the time of writing – increased beyond that assumed in the Spending Review calculations.[21] Whilst the ISC in the last Parliament had voiced concerns at the prospect of real-terms cuts, we nevertheless recognise that the Agencies have received a more generous settlement than many other areas of government spending. Effectively, these cuts will return the Agencies' funding levels to those of 2007/08 by the end of the SR10 period.[22] We will monitor the impact of this closely: where national security is concerned, funding must be sufficiently flexible to react to any significant change in the threat.



44. This Annual Report covers the Agencies' finances in detail for the 2009/10 financial year. However, given the importance of SR10, we have also questioned the Heads of the Agencies as to the likely impact of budgetary reductions on their future capabilities. GCHQ noted that:

---

[20] *We cover the outcome of this review more fully at paragraphs 162 to 167.*

[21] *Office for Budget Responsibility, 'Economic and fiscal outlook', March 2011.*

[22] *Total SIA funding (Resource DEL plus Capital DEL, less depreciation, excluding ring-fenced cyber security money) at 2009/10 prices (calculated using the GDP deflator as published on the HM Treasury website).*

Given prevailing national circumstances… it was a fair result… One of the risks would be… the whole Spending Review settlement is predicated on a rate of inflation of 1 to 2 per cent per annum… on the Treasury's assumptions; and indeed there is a risk that inflation could be substantially higher and that could have a long term effect on our funding. The other risks would be that it's dependent on a set of assumptions on how fast the internet is growing. Clearly if the internet would grow faster than those, there could still be challenges…

There is still more we can do through collaboration with our sister Agencies to try and achieve [the SR10 savings]. But certainly the challenge is going to be that much greater for the department, to make sure we are not cutting into front-line services.[23]

45. The Director General of the Security Service said that the Service could maintain key capabilities if it generates savings through increased collaborative working and internal efficiencies:

The SR settlement… represents a good outcome overall for the Service. We believe it is sufficient to carry out the Service's key functions effectively and there is nothing material to our core capabilities that we envisage we will have to stop doing. Indeed, as part of SR planning, the Service has committed to maintaining its [Counter-Terrorism] capabilities by doing more with less (in real-terms). The anticipated savings from greater collaborative working and the Living Within Our Means Programme (to keep our business as usual running costs flat) aim at enabling the Service to continue to invest in, rather than cut, the operational and technological capability we need to perform our functions effectively. Although not without risk, we have confidence in this overall strategy and do not anticipate it changing to the significant detriment of our core national security functions.[24]

46. The Chief of SIS said that the Agency had had a "*reasonable*" settlement and that SIS "*will be able to maintain our efforts on our top five priority areas*" but that they were nevertheless "*going to go through a difficult year this year*". He explained that:

*It's quite hard to… maintain the capability of the Service when we face a 10 per cent reduction in staff… I believe that we will be able to meet our present set of requirements [but] we will not be able to do as much as I would like, for example, on contributing to the global prosperity agenda, to the UK's prosperity and the global economy concerns that the Government has. It means that we are not able to increase our efforts on *** in the way that I would like to be able to increase them until our commitments in Afghanistan start to come down… The aspiration of some Ministers that we can provide answers to a whole series of intelligence requirements has to be limited, has to be contained, because we are not going to be able to do that.*[25]

---

[23] *Oral Evidence – GCHQ, 3 February 2011.*

[24] *Letter from the Security Service, 15 March 2011.*

[25] *Oral Evidence – SIS, 19 January 2011.*

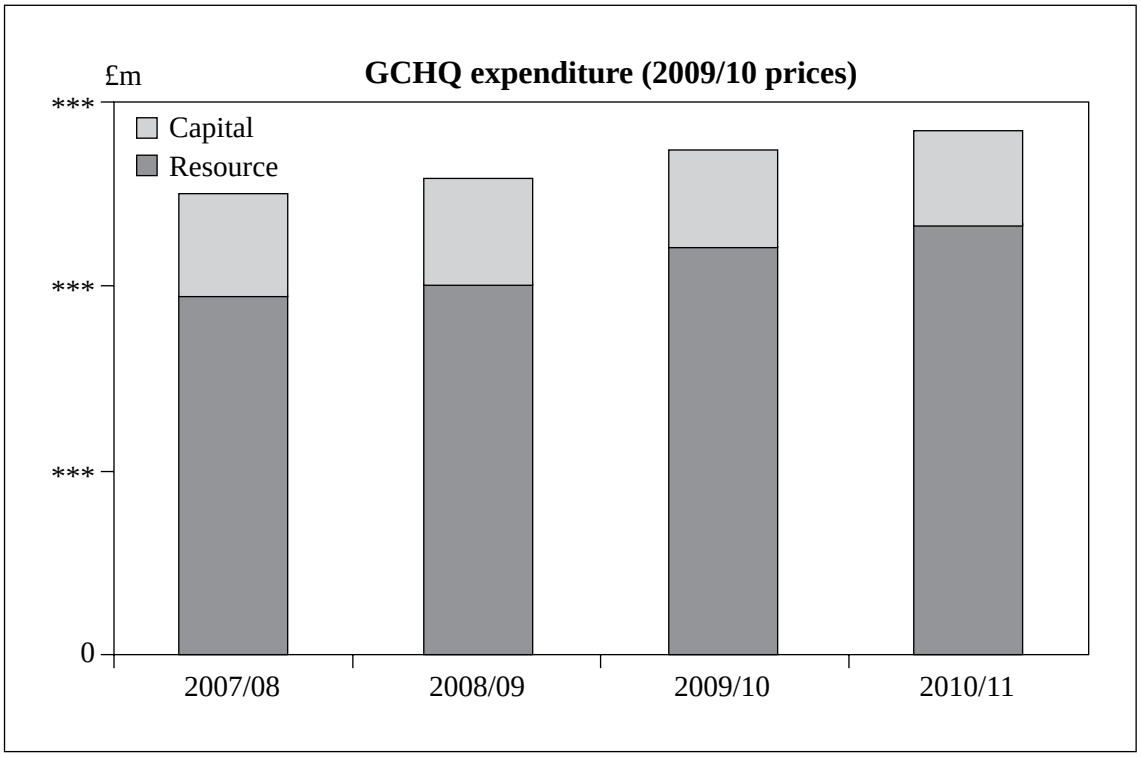
A. Given the scale of the spending cuts across government, we recognise that the intelligence and security Agencies received a fair settlement in the Spending Review. Nevertheless, we are concerned that an 11.3% reduction in budgets will inevitably have an impact on the ability of all three Agencies to maintain current levels of coverage of all aspects of the threat, and that this may worsen if inflation remains at its current levels. This will require tough decisions in the coming years.

B. Given the importance of national security work, it is essential that the Spending Review settlement can be adjusted if there is a significant change in the threat. The Committee will keep this under review.

Government Communications Headquarters

Expenditure

47. The following chart sets out GCHQ's spending over the 2007 Comprehensive Spending Review period.[26]



48. GCHQ's total expenditure in 2009/10 was £***m. This was an increase of 7.6% over 2008/09. GCHQ's total planned budget for 2010/11 was £***m (a decrease of 1.9% on 2009/10).[27]

---

[26] *Actual outturn as reported in the Consolidated Resource Accounts for 2007/08 to 2009/10. Provisional outturn for 2010/11 as reported in the unaudited Resource Accounts (due to accounting changes 2010/11 figures no longer include Cost of Capital charges). All figures adjusted to 2009/10 prices (calculated using the GDP deflator as published on the HM Treasury website).*

[27] *2010/11 nominal budget (as opposed to the figures shown in the chart above which have been deflated using the GDP deflator).*

SIGINT Modernisation Programme (SIGMOD)

49. The ISC has previously reported on GCHQ's SIGINT Modernisation Programme (SIGMOD), which GCHQ describes as "*a dynamic and inter-related group of Programmes and projects… of critical importance to the future of GCHQ*".[28] However, the Committee in the last Parliament was not satisfied with the amount of information it had been provided with concerning SIGMOD. In last year's Annual Report, it concluded: "*It is essential that [the ISC]… is given a fuller explanation of the SIGMOD programme.*"[29]

50. GCHQ this year provided the Committee with details on nine strands: Support to Military Operations; Transforming Analysis; Mastering the Internet; the National Technical Assistance Centre (NTAC); Better Business; IT Services; Facilities Management; Portfolio, Programme and Project Management Services; and Information and Communications Technology Research. The Committee was concerned as to whether some of the projects and strands under SIGMOD are directly related to modernising GCHQ's SIGINT capability. The Director acknowledged that SIGMOD:

> *has probably got the wrong label now… Increasingly the systems that we are seeking to deploy, we wish to be mission-agnostic, by which I mean I want to be able to do the SIGINT mission, but also some of the Information Assurance detection mission… the label SIGMOD, which has been catchy and may have worked in the past, will no longer be strictly accurate.*[30]

GCHQ has since clarified that it is only the first four of the nine strands listed above that make up SIGMOD, with the others instead forming part of their wider Corporate Technical Investment Portfolio (CTIP). Given that in 2009/10 GCHQ spent £***m on these projects – over ***% of the entire Single Intelligence Account – the Committee welcomes the provision of a more accurate explanation.

51. From the information that we have been provided with this year, it appears that the majority of the SIGMOD/CTIP projects are scheduled to deliver on time, and cost less than their estimated budgets. There are, however, areas where this has not been the case. In particular, delivery of a new desktop system across the GCHQ estate (a project with a forecast whole-life cost of £***m) has not met expectations. The Director has acknowledged that GCHQ was "*very disappointed*",[31] having previously hoped to have a partnership where the company "*would invest their R&D functions to potentially support SIGINT in the future*".[32] It is, in our view, most unfortunate that a project that had such long-term potential is not living up to expectations.

C. GCHQ's Corporate Technical Investment Portfolio (CTIP), of which SIGMOD is part, accounts for a significant proportion of the SIA expenditure. It is a complex set of programmes that encompasses most of GCHQ's work. The Committee has therefore tasked its Investigator to scrutinise CTIP's structure and overarching governance and report to us his findings. This investigation is now under way.

---

[28] *Written Evidence – GCHQ, 20 September 2010.*

[29] *Cm 7844.*

[30] *Oral Evidence – GCHQ, 3 February 2011.*

[31] *Ibid.*

[32] *Oral Evidence – GCHQ, 9 February 2010.*

We have also asked the National Audit Office to examine specific projects under the SIGMOD banner in due course, to assess the value for money they offer.

Policy

International Counter-Terrorism (ICT)

52. GCHQ's work on Counter-Terrorism remained steady in 2009/10 at around a third of overall effort. GCHQ reports that it put the bulk of this effort into the PURSUE strand of CONTEST[33] (namely, to stop terrorist attacks), with support for Security Service priority investigations remaining the core ICT task. Counter-Terrorism work in 2009/10 was dominated less by British Pakistani operations than in the past, with Yemen and East Africa especially prominent. GCHQ has supported Security Service investigations into Al-Qaeda in the Arabian Peninsula (AQAP) and ***. On the PROTECT strand of CONTEST, GCHQ's work has informed aviation security planning and also disrupted hostage-taking plans by ***.

53. As well as support to specific Security Service investigations, GCHQ explained to the Committee that it also conducts more strategic Counter-Terrorism work. GCHQ has described this as follows:

> *One of the capabilities that we… can bring to the table is the ability to… horizon-scan future areas, or areas where there may not be an identified threat stream today that we've successfully identified, but where one may emerge…* ***.[34]

Non-ICT work

54. After ICT, GCHQ's second largest area of effort is Asia (including Afghanistan), which accounted for ***% of effort in 2009/10, up slightly from 2008/09. Much of this work supports the British military presence, ***. GCHQ reports successes in gaining access to new sources of communication ***.

55. The other area of increased resource allocation in 2009/10 was the Middle East and North Africa, which rose to ***%. Iran and Yemen are priorities, while effort has reduced on Iraq. Levels of resource devoted to Counter-Proliferation, serious crime, Hostile Foreign Activity and electronic attack remained broadly stable in 2009/10.

56. ***.[35]

57. ***.[36]

Information Assurance (IA) and Communications-Electronics Security Group (CESG)

58. The Communications-Electronics Security Group (CESG) – part of GCHQ – provides advice and assistance on the security of communications and electronic data to

---

[33] *The Government's Counter-Terrorism Strategy (CONTEST), and its four strands, are explained further in paragraphs 150 and 151.*

[34] *Oral Evidence – GCHQ, 3 February 2011.*

[35] *Ibid.*

[36] *Ibid.*

government departments, the Armed Forces, and other public sector bodies (including the health sector and law enforcement) and those private companies that form part of the UK's Critical National Infrastructure (such as utility companies).[37] As such it is the national technical authority for Information Assurance (IA).[38] CESG operates on a cost-recovery basis, charging departments and agencies for the services it provides.

59. In last year's Annual Report, the ISC noted that the funding model for CESG's services was being reviewed. In 2009/10, CESG's total revenues for the services it provided to other departments were £***m, resulting in a shortfall against expenditure of £3.6m which GCHQ was left to subsidise. This followed a similar shortfall in 2008/09. It would appear that, across government, departments and agencies do not view investment in IA as a priority, and GCHQ is being forced to compensate for this.

60. The Committee understands that in November 2009 the IA Oversight Board, chaired by the Cabinet Secretary, acknowledged the market failure of the current model and agreed interim arrangements for 2010/11. The Director of GCHQ has told us:

> *I am personally very disappointed that we haven't been able to get satisfactory funding arrangements from other government departments over the last 18 or 24 months, where we have tried very hard with the Cabinet Secretary's support, but it has never quite come to fruition.*[39]

61. The Deputy National Security Adviser has now been tasked with identifying a future funding model that will ensure the sustainability of CESG's finances.

D. The Committee is disappointed that government departments and agencies do not view investment in Information Assurance as important, and that this has led to GCHQ having to subsidise CESG by several million pounds per year. We are concerned that there appears to have been little progress in achieving a resolution since last year. The Deputy National Security Adviser must prioritise the development of an effective funding model, which should be implemented within the next six months.

Administration

Staffing and recruitment

62. During 2009/10, 491 new staff joined GCHQ resulting in a net increase in permanent staff numbers of over 5% (from 5,393 to 5,675). In 2010/11, GCHQ intends to reduce its total number of staff through a combination of an early retirement scheme, not filling empty posts and natural wastage. It has informed the Committee that "*further staff reductions may be required during the SR10 period*".[40]

---

[37] *www.cesg.gov.uk*

[38] *'Information Assurance' relates to the integrity, confidentiality and reliability of Information and Communications Technology systems and data. As National Technical Authority, CESG advises organisations on how to manage the risks to their electronic information and services. It does this mainly through the provision of intelligence on threats and vulnerabilities, good practice security advice and technical security standards.*

[39] *Oral Evidence – GCHQ, 3 February 2011.*

[40] *Written Evidence – GCHQ, 19 January 2011.*

63. In addition to the 5,675 permanent staff, GCHQ employed 297 'time-hire'[41] contractors at a total cost of £43.1m. The average annual cost of these was £145,138, compared with an average annual cost of £44,534 for a full-time GCHQ employee. When questioned about this significant additional expense, GCHQ argued that public sector pay constraints combined with the short-term nature of some of the project work it is engaged in means it must employ some technology specialists as contractors rather than permanent staff. GCHQ also explained that it has rationalised all of its 'time-hire' contractor procurement through a single provider, who had already produced savings of £*** in the first three months of the contract, with a commitment to reduce costs further in future.

64. GCHQ employs a significant number of Armed Forces personnel for their expertise, to ensure an exchange of SIGINT skills with the Armed Forces, and also to provide a capability to deploy personnel overseas to locations where it would be difficult to send GCHQ civilian staff. This arrangement benefits both the Ministry of Defence (MoD) and GCHQ, and therefore finding suitably qualified personnel is important to both organisations. The Committee notes that the number of Armed Forces personnel employed by GCHQ has fallen over the last two years, and the MoD has not been able to meet GCHQ's requirement. In 2009/10, GCHQ employed *** Armed Forces personnel, a fall of 1.7% on 2008/09, and a 20% shortfall on the overall requirement. We are concerned that the cuts that the MoD faces as a result of the Strategic Defence and Security Review (SDSR) may exacerbate this problem. However, in the short term, with the anticipated reduction of forces in Afghanistan by 2014, there should be less need for direct GCHQ support to those forces, and therefore the requirement may decrease, as GCHQ explained:

> *I wouldn't be surprised if, given the consequences of the SDSR and SR10, that [the requirement for Armed Forces personnel] goes down a little bit. I think we have got a lot of active work under way, to look at areas where we might transfer some discrete, some specific tactical tasks back over to the single Service-funded, i.e. non SIA-funded, military manpower. We are always looking at where we can… reprioritise internally, to… use our manpower in different ways.*[42]

65. Even with this reallocation, there will still be a requirement for the MoD to provide GCHQ with Armed Forces personnel in order to provide in-theatre capability. The MoD will therefore need to prioritise this provision of personnel. A failure to do so will not just create problems for GCHQ, but also bring increased risks for the Armed Forces in terms of reduced SIGINT expertise for intelligence specialists.

---

[41] *'Time-hire' contractors are individuals employed on a daily basis to perform specific functions.*

[42] *Oral Evidence – GCHQ, 3 February 2011.*

66. In terms of new recruits, GCHQ generally met its targets in 2009/10, except for linguists where recruitment of sufficient numbers of staff with rare languages remains challenging. In an attempt to overcome this, GCHQ has established, in conjunction with the other Agencies, a joint language centre hosted by the Security Service "*to provide… a coherent tri-agency rare language capability; ****".[43] ***. The Director also told us that he was "*quite open to [taking] a hard look at some of the nationality rules*"[44] around linguists in order to make recruitment of those with rare languages easier.

67. The Director has noted that retaining sufficient numbers of suitably-qualified internet specialists also remains a difficulty, telling us:

> *I need some real internet whizzes in order to do cyber and I am not even sure they are even on the contractor market, so I need to work on that. They will be working for Microsoft or Google or Amazon or whoever. And I can't compete with their salaries; I can offer them a fantastic mission, but I can't compete with their salaries. But I probably have to do better than I am doing at the moment, or else my internet whizzes are not going to stay… and we do have a steady drip, I am afraid. Month-on-month, we are losing whizzes who'll basically say: 'I'm sorry, I am going to take three times the salary and the car and whatever else'.*[45]

E. We are concerned about GCHQ's inability to retain a suitable cadre of internet specialists to respond to the threat. We therefore urge GCHQ to investigate what might be done within existing pay constraints to improve the situation. We also recommend that the Cabinet Office – as lead department for cyber security – considers whether a system of bonuses for specialist skills, such as exists in the United States, should be introduced.

68. GCHQ's Cabinet Office Capability Review, which was published in July 2009, reported that GCHQ's "*delivery against diversity targets is poor*" and that "*[it] needs to understand better the reasons underpinning performance in this area, and the Board must take responsibility for greater improvement.*"[46] GCHQ was also the subject of adverse media coverage following the leaking of the conclusions of an internal review criticising the Agency's record in this area. The Director told us that:

> *Some of the people who were most annoyed about that were our own [Black and Minority Ethnic (BME)] network, interestingly, who said that they did not accept the picture… I actually think it has been taken very seriously [by the Board], but there are some iconic, symbolic, very visible steps to take which will then have a ripple effect.*[47]

---

[43] *Ibid. See also paragraph 101.*

[44] *Oral Evidence – GCHQ, 3 February 2011.*

[45] *Ibid.*

[46] *GCHQ: Baseline Assessment, July 2009.*

[47] *Oral Evidence – GCHQ, 3 February 2011.*

69. In response to the Review, the GCHQ Board agreed a set of 17 diversity initiatives aimed at improving performance in this area, including mandatory diversity training for all staff, awareness-raising events, and consulting other organisations to identify best practice.[48] At 1 March 2011, the number of BME junior and middle managers had increased very slightly from 2.5% to 2.85% of the workforce. GCHQ assesses that "*there is an increasingly positive attitude towards diversity in the department and a lot of effort and momentum to improve the culture and workforce balance*".[49]

Accommodation

70. GCHQ's expansion over the CSR07 period, due to new demands (primarily on Counter-Terrorism), put pressure on its available accommodation, and over the past four years it has taken the following steps to mitigate this:

- In 2007, it decided not to proceed with the disposal of its Oakley site after its main Benhall location proved too small for the growth in staff numbers it was experiencing (Oakley was originally to be disposed of as part of the Private Finance Initiative (PFI) deal which saw Benhall constructed).[50]
- In September 2009, GCHQ obtained planning permission to expand further the available accommodation at Benhall.
- In March 2010, when these expansion plans proved unaffordable, GCHQ purchased a new site in the Cheltenham area with associated contracted services (at an approximate total cost of £40m) in which to house its contractor staff.
- In March 2011, GCHQ announced that, given the planned reduction of staff over the SR10 period, and the opening of the new site, the Oakley site will, after all, be closed in 2012.

However, GCHQ told the Committee in March 2011 that Benhall will still be running at full capacity after the closure of Oakley, and that if the headcount were to increase they would again need to seek additional accommodation.[51]

71. In addition to these changes in Cheltenham, GCHQ has made the decision to dispose of its London office, and instead use available space either with SIS or the Security Service. The Committee was told in evidence this year that this process was expected to start in four or five years.

---

[48] *Written Evidence – GCHQ, 23 March 2011.*

[49] *Ibid.*

[50] *Cm 7807.*

[51] *Written Evidence – GCHQ, 23 March 2011.*

F. The Committee welcomes the savings that will accrue from the disposal of GCHQ's London office and Oakley site. However, we remain concerned that GCHQ's accommodation strategy has been haphazard in the past and, with the current rationalisation taking place, lacks any flexibility for the future. The GCHQ Board must plan better for the future and develop a sensible long-term strategy for its accommodation requirements.

Asset management

72. In its 2008–2009 Annual Report, the ISC criticised GCHQ as having had a "*cavalier attitude towards valuable and sensitive assets*", particularly around the control of laptops. In its management letter for the same period, the National Audit Office noted that asset management was a problem, with an internal GCHQ audit failing to account for 34% of 26,860 items in its stores. In 2009/10, the Director of GCHQ stated that he would be "*directing progress on [this issue] which [has] been highlighted… as of concern*".[52]

73. GCHQ has told us that the missing items were not fixed assets, and included tools, clothing and commercially-available communications equipment, with a total estimated value of no more than £1m. Since this represented equipment that could not be accounted for over a ten-year period, this did not have a material effect on GCHQ's accounts. There was also a balance to be struck against the time and money that would need to be spent to locate the equipment. GCHQ has ascertained that 95% of the missing items would present no security risk should they be lost, but had concluded that it was more likely that they had been destroyed and poor record keeping meant that this had not been noted. The inability to locate these assets did not appear to have had an impact on operational activity. GCHQ told us:

> *What we believe has happened over a number of years is the equipment has been issued from the stores to deployment, primarily to places like Afghanistan and Iraq, and it has not been adequately updated in the records. So the people who are running the systems have not expressed concerns that they have not been able to find the equipment. They have just been not very good at their reporting.*[53]

G. The Committee is concerned that, over a prolonged period, GCHQ has been unable to account for equipment worth up to £1m. Assets must be monitored effectively and controls must be in place to ensure that public money is not wasted. Whilst the majority of the items that could not be traced attracted no security risk, GCHQ has admitted to us that it cannot guarantee that this is the case for 5% (or 450) of these items. Although the Committee has no reason to believe national security has been compromised, the Agencies must do all they can to avoid the loss of potentially sensitive equipment. The public interest requires that GCHQ learns from the repeated mistakes of the past. The Committee expects GCHQ to ensure that the situation does not arise again.

---

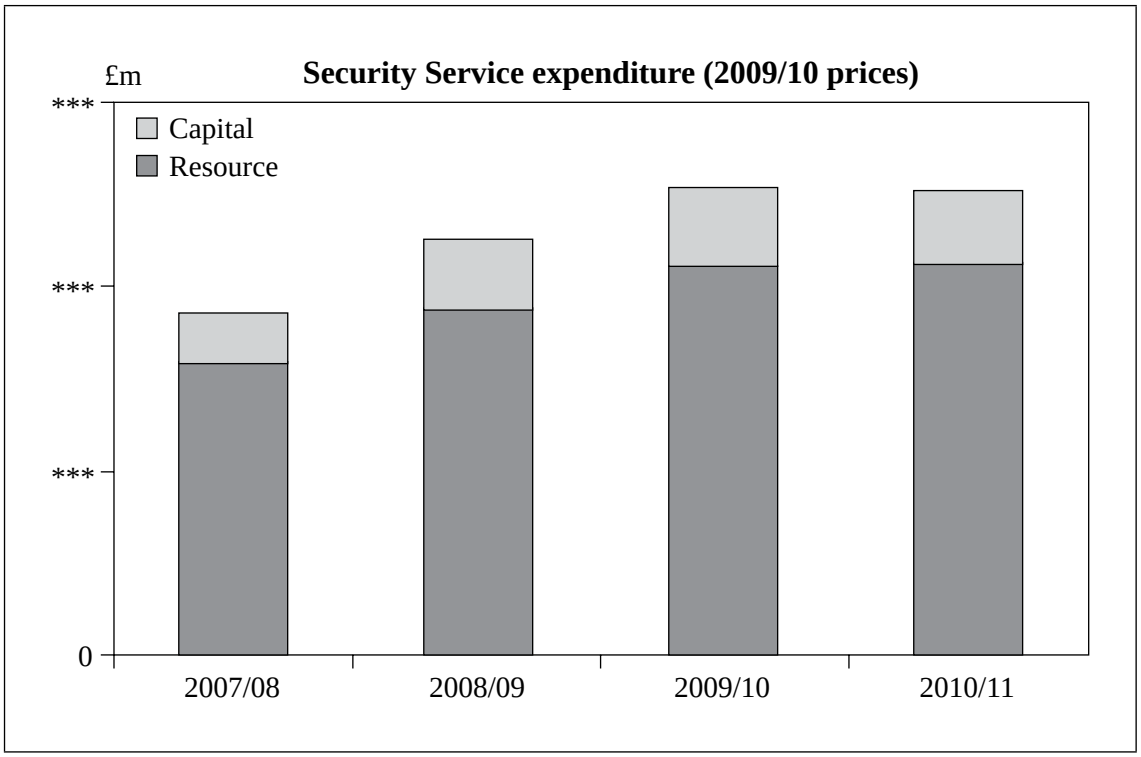
[52] *GCHQ Annual Report and Resource Account 2009/10.*

[53] *Oral Evidence – GCHQ, 3 February 2011.*

The Security Service

Expenditure

74. The following chart shows the Security Service's spending over the four years of the CSR07 period:[54]



75. The Security Service's total expenditure in 2009/10 was £***m. This was an increase of 14% over 2008/09. The Security Service's total planned budget for 2010/11 was £***m (an increase of only 3.8% on 2009/10).[55]

76. Commenting on its performance, the Service explained that 2009/10 had seen an additional demand on resources given the need to respond to increased legal scrutiny – including a judicial review and police investigation – as well as dealing with the continued high levels of terrorist threats. Despite these challenges, the Service noted that "*performance against the [CSR07] plans remained firmly on target*".[56]

---

[54] *Actual outturn as reported in the Consolidated Resource Accounts for 2007/08 to 2009/10. Provisional outturn for 2010/11 as reported in the unaudited Resource Accounts (due to accounting changes 2010/11 figures no longer include Cost of Capital charges). All figures adjusted to 2009/10 prices (calculated using the GDP deflator as published on the HM Treasury website).*

[55] *2010/11 nominal budget (as opposed to the figures shown in the chart above which have been deflated using the GDP deflator).*

[56] *Security Service Resource Account 2009/10.*

National Audit Office findings

77. In its examination of the Security Service 2009/10 Accounts, the National Audit Office (NAO) identified two substantive financial reporting issues. First, there was a pronounced surge in the Service's expenditure towards the end of the financial year. For example, 59% of the spend on 'Assets in the Course of Construction' was spent in the last three months of the financial year. Similarly, approximately 40% of the Service's budget for interception, operational equipment and systems was spent in the same period. The NAO noted that such 'end-year surges' in spending considerably increase the risk of inefficiency and lack of value for money. They recommended that the Service "*[pays] greater attention to the forecasting process and to managing an even spread of expenditure through the financial year*".[57] When the Committee questioned the Director General on this issue, he told the Committee that:

> *We are, I think, making some progress in this area. We recognise the risks of this in that people may feel, 'I've got money, so I'll spend it', rather than thinking about what the value is. But if you look at the figures for the current year, we are in a very much better position in terms of end-year surge than we were previously.*[58]

H. The Committee welcomes the improvement by the Security Service in managing 'end-year surges'. However, we urge the Service to implement the recommendation of the National Audit Office to improve their forecasting processes in order to manage expenditure evenly throughout the financial year.

78. The second major issue identified by the NAO concerned the Service's classification of staff numbers and costs: this is the third year in a row that the NAO has found fault with the Service in this area. A lack of clear definitions, and consistency in their application, meant that reported staff costs were not accurate, particularly in respect of consultants and contractors. Whilst inaccurate staff classification is largely a technical issue, it nevertheless means that the Service does not have a proper understanding of its headcount, which makes it much more difficult to plan effectively and also to target efficiency savings.

Technology

79. The Director General told the Committee that much of the Service's additional funding from CSR07 was being invested in technology. He explained that this was to ensure that:

> *Our technology was in a better state than it had been in 2000 to 2005, when, not to put too fine a point on it, we were in a bit of mess really. We are in a much better position now, although there are still some quite serious challenges around it, both in terms of stability and in delivering the last bits of our ambitions on the ability to move around our information and bring together our information.*[59]

---

[57] *National Audit Office, 'Management Letter on the audit of the 2009–10 financial statements', August 2010.*

[58] *Oral Evidence – Security Service, 9 February 2011.*

[59] *Ibid.*

80. This technological investment was focused on both improving operational capability and strengthening information handling and processing. This latter point is particularly important for the Service, especially in relation to its record-keeping systems, and is something that the ISC commented on in the last Parliament. (The issue of record keeping has arisen once again in relation to the Inquests into those who died in the 7/7 bombings – paragraphs 238 to 244.)

81. This increased focus on technology is reflected in the following four major capital projects during 2009/10:

i. The IQ Programme: this is a major programme with delivery costs of £***m. It is intended to transform the way in which the Service manages investigations and processes its intelligence, significantly improving large parts of the investigative process.

ii. The Infrastructure Portfolio: this has delivery costs in excess of £***m and the Service describes it as "*underpinning everything that we do*".[60] The 'Portfolio' includes a number of sub-projects including Applications Hosting and Storage (AHS), the Networks Programme, and the Joint Data Centre with SIS.[61] One of the strands – the Networks Programme – has seen costs escalate this year by 43% (to £***m). When questioned, the Service explained that the increase was due to changes in the scope of the programme and difficulties in scheduling work so as to minimise disruption.

iii. The Digital Intelligence Programme (DIGINT): DIGINT was established in 2009 with the goal of allocating more staff to use more (and improved) technology for digital intelligence gathering and analysis, and devoting more resources to technological research and development. DIGINT is expected to cost £***m to deliver (11.6% less than the original business case).

iv. The Security Service's new electronic information management system[62] is intended to "*modernise and enhance the Service's information management capability*" and "*provide a greater level of information assurance and mitigate the risks of intelligence failure and information loss*".[63] The Director General told the Committee in evidence that the project "*is in some difficulties*".[64] We have subsequently been told that "*given the clear priority of ensuring the stability of our IT systems ahead of the Olympics*" the Service had taken the decision to "*delay the 'go-live'… until after the 2012 Olympics*".[65]

---

[60] *Letter from the Security Service, 16 September 2010.*

[61] *The Joint Data Centre is covered further at paragraphs 263 to 265.*

[62] ***.

[63] *Letter from the Security Service, 16 September 2010.*

[64] *Ibid.*

[65] *Letter from the Security Service, 8 April 2011.*

Policy

International Counter-Terrorism

82. The Security Service allocated 72% of its overall resources to International Counter-Terrorism (ICT) during 2009/10. This was down from 75% in the previous year, largely due to a significant reallocation of resources to Northern Ireland. However, the Service's spending on ICT increased by 11.6% (to £***m).

83. The Director General told us that "*as of today, we are in a situation where the threat from international terrorism remains serious*".[66] In February 2011 he said: "*The amount of surveillance that we undertook [in ***] with police colleagues was the highest at any point that we have ever had to put out on the streets.*"[67]

84. The increase in resources has enabled the Service to "*keep pace*"[68] with the ICT threat. The Service reports that it is:

> *... continuing to increase our capability to detect plots before they come to fruition. We have increased the amount and impact of *** and built and consolidated a regional network enhancing co-operation with police.*[69]

85. The Director General explained that the Service was continuing to see a diversification in the threat from Al-Qaeda and its associated organisations. In particular, there has been a move away from the pre-eminence of Al-Qaeda Core based in the Federally-Administered Tribal Areas (FATA) of Pakistan, with an increased threat emanating from Al-Qaeda in the Arabian Peninsula (AQAP) and especially from Yemen. This threat was seen in the attempted attack on an aircraft bound for Detroit on Christmas Day 2009 and the two printer cartridge bombs detected at East Midlands and Dubai airports in October 2010. The Director General told us that "*Al-Qaeda in the Arabian Peninsula and other franchise operations are clearly energetic and creative*".[70]

86. In 2010/11, the relative allocation of effort on ICT remained at around 72%; however, an overall increase in budgets meant that expenditure on ICT rose by 9% to £***m.[71]

Northern Ireland-Related Terrorism

87. As was seen from the murder of Police Constable Ronan Kerr by a car bomb in Omagh on 2 April 2011 and the discovery of a 500lb bomb near Newry on 7 April, Northern Ireland-Related Terrorism (NIRT) continues to pose a very real threat. The Service told us that:

> *The threat posed by republican terrorist groups, both in terms of the number of attacks attempted and the critical mass of individuals involved in terrorist activity, continues to rise.*[72]

---

[66] *Oral Evidence – Security Service, 9 February 2011.*

[67] *Ibid.*

[68] *Letter from the Security Service, 16 September 2010.*

[69] *Ibid.*

[70] *Oral Evidence – Security Service, 9 February 2011.*

[71] *Budgeted, not yet audited.*

[72] *Letter from the Security Service, 16 September 2010.*

88. ***.[73]

89. In Northern Ireland itself, the threat level remained at "SEVERE"; however, the threat level in the rest of the UK was raised to "SUBSTANTIAL" on 24 September 2010. The Director General told us that "*We don't have any reason to believe that an attack here [UK mainland] is imminent, but I certainly believe it's in their minds*".[74]

90. In 2008/09, the Service's effort on NIRT had decreased to 13% of overall effort. As a result of the deteriorating security situation in Northern Ireland, during 2009/10 the Service reappraised effort in this area, and increased allocation of resources on NIRT to 15%. In financial terms the Service's funding of NIRT increased by 34%, bringing the total to £***m.

91. Although this urgent reallocation of resources has proved disruptive to the Service's overall plans, the Service has told us that it was having "*a disproportionately great effect in improving our intelligence capacity in Northern Ireland*".[75] However, the Service still assessed that ***.[76]

I. The Security Service has told the Committee that it has been able to respond effectively to the recent increased threat in Northern Ireland. Nevertheless, given the increase in the number of attacks, it is clear that further sustained effort will be required. In the context of declining resources, this will affect the Service's capability in other areas, which is a matter for concern.

Hostile Foreign Activity

92. In 2009/10, effort on countering Hostile Foreign Activity was 4% (equating to approximately £***m in financial terms, which was 27% more than in 2008/09). The Security Service has told the Committee that the main threats continue to be posed by Russia and China.[77] During 2009/10, high-profile events such as the expulsion of a Russian diplomat in December 2010, the intention to deport – on national security grounds – a Russian national working as a Parliamentary researcher, and the Anna Chapman spy ring discovered in the US demonstrated Russia's continuing espionage activity against the UK and its allies.

Olympics

93. In his public speech to the Worshipful Company of Security Professionals in September 2010, the Director General stated that:

> *The eyes of the world will be on London during the Olympic period and the run up to it. We have to assume that those eyes will include some malign ones that will see an opportunity to gain notoriety and to inflict damage on the UK and on some other participating nations.*[78]

---

[73] *Oral Evidence – Security Service, 9 February 2011.*

[74] *Letter from the Security Service, 16 September 2010.*

[75] *Ibid.*

[76] *Oral Evidence – Security Service, 9 February 2011.*

[77] *Letter from the Security Service, 16 September 2010.*

[78] *Director General of the Security Service, speech to the Worshipful Company of Security Professionals, 16 September 2010.*

94. The Service has told us that the Olympics are "*central to our strategic planning for the initial phase of the SR period*".[79] In November 2010, the Committee was informed that the Security Service will be seeking to recruit 100 new intelligence officers by November 2011 in time for the Olympics[80] – the Service has subsequently informed us that 90% of these are expected to have taken up their posts by November 2011.[81] Overall, the Director General assessed that the Service was well placed to manage the risks that the Olympics will bring.

95. This focus on the Olympics will inevitably have worrying consequences for the rest of the Service's work. The Director General told us that:

> *It's a huge event, and might have really big security implications… we are going to be pulling at least 150 intelligence staff out of other roles across the Service to put them back into intelligence work at the front line, and possibly 300, which will basically close half of what we are doing in other areas. ***… So there will be a large diversion of resource from other things into the Olympics. But I don't think we've got any option about that.*[82]

The Security Service has subsequently told us that it expects it will need to *** during the Olympics.

J. The Service is already focused on planning around the 2012 Olympic Games. The Director General has told us that he considers the Service to be well-placed to manage the risks that the Olympics will bring. The Committee is nevertheless concerned that this will inevitably divert resources from the Service's other work during this period, and thus expose the UK to greater risk. The National Security Council must take such steps as are necessary to minimise the risk to the UK.

Administration

Staffing and recruitment

96. Between April 2006 and April 2009, the Security Service's staffing levels increased by just under 40%. In 2009/10 the rate of growth was substantially less, however, with an increase of only 6.8%. Staff numbers as at April 2010 were 3,685.

97. This figure was originally planned to increase to 4,100 by April 2011. However, given the current financial climate, the Service took the decision in November 2009 to restrict growth to 3,800. As at April 2011, staff numbers were 3,604. The Service told the Committee that it intends to "*use this opportunity to become the 'right 3,800' through staffing critical growth areas*" and also to "*expand the pool of widely deployable front line operational and investigative staff*".[83] Over the course of the SR10 period, however,

---

[79] *Letter from the Security Service, 14 March 2011.*

[80] *Cabinet Office Monthly Update, November 2010.*

[81] *Written Evidence – Security Service, 5 May 2011.*

[82] *Oral Evidence – Security Service, 9 February 2011.*

[83] *Letter from the Security Service, 16 September 2010.*

with the additional funding for cyber security and following the Government's review of Counter-Terrorism powers, the Director General acknowledged that "*we might well be moving up towards the 4,000 figure by the end of the [SR] period.*"[84]

98. These changes are being managed under the Service's 'Living Within Our Means' programme. The Director General told us that the aim of this programme was to "*continue to grow capability, but without increasing the cost of running the service on a day-to-day basis*".[85] The programme is forecast to save around £110m between 2011/12 and 2013/14, with the single biggest saving (nearly half the total) projected to come from limiting the growth of the Service to 3,800 in the first few years of the SR10 period.

99. In order to help achieve these savings, the Service has introduced a 'managed exit' programme. Last year the Director General told the Committee that:

> *There will be a mixture of voluntary and compulsory redundancies in the Service, and I want to try and put the Service, in the next 12 months, into a better position as we go into what are likely to be tougher times.*[86]

100. By March 2011, a total of 216 staff had left the Security Service under this 'managed exits' programme. Of these staff, 103 left under voluntary severance terms and 113 were redundancies (all but two of these were voluntary).[87] The Service has told us that:

> *Our work to reshape the Service and to achieve the 'right 3,800' has given us more headroom to retain, recruit and develop those staff with the skills we need to expand our capability and capacity in business critical areas.*[88]

101. During 2009/10 the Security Service ran a number of recruitment campaigns, prioritising graduate intelligence officers, operational intelligence officers, intelligence analysts, digital intelligence (DIGINT) specialists and critical linguist posts. The Service says that it had "*significant success against the intelligence and DIGINT [recruitment] requirements*" although "*the traditionally difficult area of critical linguist posts remained challenging*".[89] The combination of the establishment of a joint language centre (a collaborative venture with GCHQ and SIS[90]) and a new pool of linguists has significantly eased the problem. However, this remains a top priority for further recruitment.

102. The Security Service's total expenditure on consultants (including the use of interim specialists and contractors) during 2009/10 was £56.8m – an increase of 73.5% on 2008/09. This was despite the Committee being told last year that the Service was reviewing its use and management of consultants and contractors and that this review would deliver benefits in the second half of 2009/10. The vast majority (82%) of the Service's total expenditure on consultants and contractors is IT-related. The Service has told the Committee that this is due to the need for technical expertise to deliver its major

---

[84] *Oral Evidence – Security Service, 9 February 2011.*

[85] *Oral Evidence – Security Service, 26 January 2010.*

[86] *Ibid.*

[87] *Letter from the Security Service, 14 March 2011.*

[88] *Ibid.*

[89] *Letter from the Security Service, 16 September 2010.*

[90] *Further information on the work of the joint language centre is at paragraph 66.*

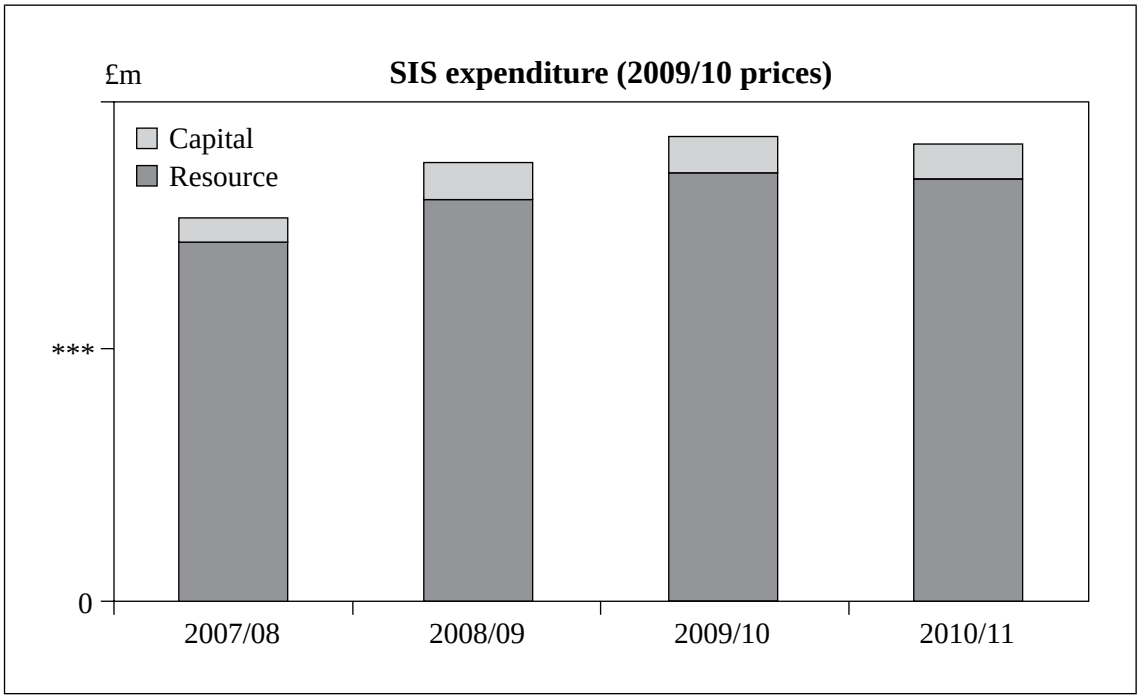
IQ and Network Infrastructure projects.[91] Looking ahead, the Service expected that the overall cost of consultants and contractors for 2010/11 would rise by a further 52%. We have since been told that efforts within the financial year to cut these costs are likely to have had the effect of reducing the extent of the increase.[92]

K. The Committee recognises that the Security Service needs IT specialists in order to deliver its major technology projects. However, spending on consultants and contractors continues to increase at a significant rate. The Service should consider whether collaborative working – with GCHQ in particular – could provide some savings in this area. The Committee will examine the Agencies' use of consultants and contractors in greater detail over the coming year.

The Secret Intelligence Service

Expenditure

103. The following chart demonstrates growth in SIS's spending over the 2007 Spending Review period.[93]



Financial management

104. SIS's total expenditure in 2009/10 was £***m. This was an increase of 9.9% over 2008/09. SIS's total planned budget for 2010/11 was £***m (an increase of 2.4% on 2009/10).[94]

---

[91] *Letter from the Security Service, 16 September 2010.*

[92] *Final figures for 2010/11 have not yet been audited.*

[93] *Actual outturn as reported in the Consolidated Resource Accounts for 2007/08 to 2009/10. Provisional outturn for 2010/11 as reported in the unaudited Resource Accounts (due to accounting changes 2010/11 figures no longer include Cost of Capital charges). All figures adjusted to 2009/10 prices (calculated using the GDP deflator as published on the HM Treasury website).*

[94] *2010/11 nominal budget (as opposed to the figures shown in the chart above which have been deflated using the GDP deflator).*

105. In 2008/09, SIS failed to manage its capital spend across the financial year, with a considerable 'end-year surge' which the ISC criticised. However, 2009/10 saw another 'end-year surge' in capital expenditure: two-thirds of this £***m budget was spent in the last two months of the financial year. The NAO reported that they "*remain concerned… over the level of spend close to the year-end*" – although they did not raise any concerns over the "*appropriateness of the expenditure concerned*".[95] During evidence, the Committee questioned SIS on this apparent lack of financial planning and the Chief told us that:

> *It's a reflection of the way in which in recent years the Treasury has focused on year by year accounting and budgeting without end-year flexibility. That has meant that all the money you have in one year has to be spent by the end of March. So you tend to plan at the beginning of the year and spend at the end of the year. But the degree of the surge shows an imbalance in planning, and I've been very conscious of that. I have driven the finance team and the procurement team very hard to have a more even spread of spending during the course of the year, so we don't have that peak. The Finance Director and his team have responded very effectively to that… so that this year, for example, we are on target for our profile of spend throughout the year.*[96]

L. This is the fourth consecutive year that SIS has failed to manage its expenditure effectively throughout the year and has seen an 'end-year surge'. The Intelligence and Security Committee has consistently been critical of this, agreeing with the National Audit Office's view that it increases the risk of inefficiency and lack of value for money. The Committee expects SIS, in the current financial climate, to ensure that it manages its budget sensibly in future and will monitor whether this is happening during the current financial year.

106. Bearing these issues in mind, the Committee has closely examined the expenditure on, and performance of, SIS's major capital projects. We questioned SIS in detail on their IT Programme, which is intended to deliver "*enhanced data exploitation and connectivity with partners [across the intelligence community]*"[97] and is made up of:

- the Joint Data Centre (with the Security Service, to provide secure storage outside London for their data);[98]
- Station Communications (to deliver improved communications between Head Office and stations and also within stations); and
- ***.

107. Other major capital projects include the UK Estates project (upgrading Headquarters and disposing of additional buildings) and a project to provide covert communications in ***. The projects are all to be delivered over the 2010 Spending Review period.

---

[95] *National Audit Office, 'Management Letter on the audit of the 2009–10 financial statements', August 2010.*

[96] *Oral Evidence – SIS, 19 January 2011.*

[97] *Written Evidence – SIS, 15 September 2010.*

[98] *The Joint Data Centre is covered further at paragraphs 263 to 265.*

108. The Committee questioned the Chief about the benefits that he has seen so far from these capital projects and he told us that:

> *We have had a complete upgrade of the communications of all stations around the world with Head Office, which has made it both more robust and given much greater access to their own data, historic data, so that we have better access to knowing what we actually know already, without having to find it out again. That has been a big step forward, and the connectivity between stations and Head Office has been a big step up.*
>
> *In the last financial year [we have] re-opened stations in places like ***. This year we are opening stations in ***.*
>
> *We have upgraded and expanded stations in a number of places. ***; these are examples of places where we have done that to accommodate increased numbers of staff, either by SIS or staff that were seconded by other agencies as part of their own deployment.*[99]

Foreign and Commonwealth Office (FCO) settlement

109. SIS identified total efficiency savings of £28.1m in 2009/10. The largest single saving came from a reduced annual settlement cost with the Foreign and Commonwealth Office (FCO) – this is the payment made by SIS to the FCO in return for the FCO hosting SIS stations overseas. Until 2009/10, the settlement was a notional figure, agreed in 1998, of £***m. The Chief told us "*we have been able to drive down the costs by a more accurate focus on what the extra cost of having SIS stations actually is on the Foreign Office system*".[100] SIS has informed the Committee that they agreed a revised settlement for 2008/09 and 2009/10 which was over 25% lower than the previous figure.[101]

Policy

110. When the Committee questioned the National Security Adviser about the Agencies' capabilities for dealing with the current threats, he emphasised the need for SIS to maintain flexibility:

> *[The other increasing challenge] is the importance, particularly for SIS, of maintaining coverage in as wide a range of countries as possible, given that threats are very fleetfooted at the moment, and they need to be able to turn on intelligence coverage in places like Somalia or Yemen or the Sahel or the Maghreb as the threat moves. That, I think, given the concentration that they have in the areas of highest priority… is a real issue for them.*[102]

---

[99] *Oral Evidence – SIS, 19 January 2011.*

[100] *Ibid.*

[101] *Written Evidence – SIS, 11 May 2011. This will rise by approximately 20% in 2010/11 due to increasing numbers of staff posted overseas and the effects of the fall in the value of the pound.*

[102] *Oral Evidence – SIS, 19 January 2011.*

111. Whilst just over ***% of SIS's allocation of effort is on Counter-Terrorism and Counter-Proliferation work, the remaining effort is dedicated towards maintaining a global coverage.[103] The top priorities during 2009/10 were ***. In order to maintain its global coverage, SIS has *** staff[104] in *** stations around the world. The biggest overseas stations are ***. Some stations have increased this year to deal with the growing threat (***). In contrast, SIS closed *** of its stations between 2009 and 2011 to respond to a change in the threat. These included several regional locations in Iraq.

International Counter-Terrorism

112. In terms of overall allocation of effort, SIS's highest priority remained Counter-Terrorism, which accounted for 35.9% of its resources. In 2009/10, this represented a 4% relative decrease compared with 2008/09, although the overall increase in SIS's budget meant that spending in this area increased slightly.

113. SIS told us that the ICT threat is evolving, but that they were able to keep abreast of the scale of the challenge. With their global coverage and network of foreign liaison partnerships, they regard the threat as "*broadly contained*".[105] The importance of international partnerships can be clearly seen from events in 2009/10 such as the planned Mumbai-style terrorist attack in Europe (which the UK learnt of from *** intelligence), and the interception of the printer cartridge bomb on the cargo flight passing through East Midlands Airport (which was based on *** intelligence).

114. In addition to effort on Counter-Terrorism, SIS also allocated ***. The Chief explained that:

> *Our station in *** operates both against the Counter-Terrorism target and against the [country] target. So when we compile these statistics, we will ask our station… and our teams back in Head Office, are you focused on the terrorist target or are you focused on acquiring intelligence on [the country], and the figures reflect that. So there's not duplication between these.*[106]

115. In terms of future allocation, the Chief highlighted the impact of the Olympic Games in London next year:

> *Much of this [maintaining efforts on our five top priority areas] will depend on what happens on the Counter-Terrorism front, where a third of our operational staff are committed to Counter-Terrorism work, and there will be a surge on that in the six to nine months running up to the Olympics. We are working out exactly what that extra commitment on Counter-Terrorism requirements will be… [It] will certainly have an impact on our intelligence operations and intelligence coverage of other targets during that period.*[107]

---

[103] *This geographical effort can also contribute to the thematic targets.*

[104] *Staff on substantive overseas postings or on temporary duty postings lasting over four months, not including seconded or loaned-in staff.*

[105] *Oral evidence – SIS, 19 January 2011.*

[106] *Ibid.*

[107] *Ibid.*

Non-ICT work

Iran

116. SIS allocated ***% of effort on Counter-Proliferation work and also ***% on Iran. The two targets are complementary: ***. It appears that the collective impact of the work of intelligence agencies, and others, together with international sanctions, has been to delay progress on the Iranian nuclear programme.

China

117. SIS told us that the Chief has made a commitment to visit China annually in order to build up the relationship and develop the understanding that will be required for the decades ahead in order to promote closer work on intelligence and national security subjects of mutual UK and Chinese interest. ***.[108]

118. ***.[109, 110]

Organised crime

119. Historically SIS devoted a small percentage of effort to work on organised crime. In 2006 the Serious Organised Crime Agency (SOCA) took over responsibility for this work. The Committee questioned SIS as to whether they continued to devote any effort to criminal work. The Chief told us that this was an area currently under review:

> *SOCA is the agency which has taken over responsibility for serious organised crime internationally as well as domestically. There's a debate as to whether that is the best arrangement. The Government has come up with plans for a different approach to this. We will need to see what sort of contribution we can make to that, but we don't see SIS being the lead agency for international serious organised crime. If we did, then we would need to have some reorganisation to achieve that.*[111]

Administration

120. In 2009/10, staff numbers increased by 10% over 2008/09. However, growth in staff numbers in 2010/11 was expected to fall to 2%. This reflects the decision taken by SIS in April 2010 to reduce its original target from 2,800 to 2,680, on the grounds that it was "*unaffordable*".[112] The implications of the SR10 settlement are still being worked through but are likely to mean that SIS is "*going to have to end up at 2,400*".[113] SIS has already begun planning for this with a voluntary exit scheme.

121. In January this year, the *Mail on Sunday* alleged that "*Britain's spy chiefs are to receive a lucrative multi-million-pound redundancy pay-out, despite the Government's*

---

[108] *Ibid.*

[109] ***.

[110] ***.

[111] *Oral Evidence – SIS, 19 January 2011.*

[112] *Ibid. During the course of 2010/11 this was subsequently amended to 2,600.*

[113] *Ibid.*

cutbacks".[114] The Committee questioned the Chief about the redundancies. SIS said that it had applied the early release compensation scheme before the new rules came into force in order to achieve Senior Civil Servant reduction targets of 20% between 2009 and 2011. However, the Chief stated that the sums paid to the staff leaving were much less than those alleged in the *Mail on Sunday*.[115]

122. On 31 January 2011, SIS launched a pilot 'Contact Us' facility on their public website, allowing members of the public to submit offers of service or information. ***. The new online capability will enable individuals to contact SIS who might otherwise not have been able to do so. SIS is currently evaluating the success of this facility, and we will provide an update in our next Annual Report.

123. In March 2010 Daniel Houghton, a former SIS member of staff, was arrested and charged with theft and offences under the Official Secrets Act (OSA) following an investigation led by the Metropolitan Police and the Security Service. Mr Houghton had attempted to sell electronic files containing secret technical data and staff lists to a Dutch intelligence service. The Dutch contacted the Security Service which was then able to contain the damage to UK national security. Mr Houghton pleaded guilty to the two OSA offences on 14 July 2010 and was sentenced to 12 months' imprisonment on 3 September 2010. SIS is currently carrying out a 'lessons learned' exercise to review its recruitment procedures, vetting, in-career security management, physical security and information assurance, including electronic media security.

Death of Gareth Williams

124. Gareth Williams was a GCHQ officer on secondment to SIS in London. In August 2010 his body was discovered inside his flat in central London in suspicious circumstances. The precise cause of Mr Williams' death remains unclear, and the police are continuing to investigate. At the time of writing, the Inquest into Mr Williams' death has not yet reported.[116]

[114] *Mail on Sunday article, 30 January 2011.*

[115] *Letter from SIS, 28 February 2011.*

[116] *The Committee does not intend to comment on the matter at this time.*

SECTION 5: WIDER INTELLIGENCE MACHINERY

Central structures, strategies and responsibilities

The National Security Council

125. Following the general election in May 2010, the Prime Minister announced the creation of a National Security Council (NSC) and the appointment of a National Security Adviser (NSA) to oversee all aspects of national security.[117] The NSC – which meets weekly – co-ordinates the work of those departments and agencies that are involved in dealing with national security issues, including the FCO, MoD, Home Office, Department of Energy and Climate Change and the Department for International Development. This is reflected in the membership of the NSC: chaired by the Prime Minister, its permanent members are the Deputy Prime Minister, Chancellor of the Exchequer, Foreign, Home, Defence, Energy and Climate Change and International Development Secretaries, and the Minister for Government Policy and Security Minister, with other Cabinet Ministers attending as required. The Chief of the Defence Staff, Chairman of the JIC and Heads of the intelligence and security Agencies also attend.

126. Three Ministerial sub-committees were established beneath the NSC with a remit to examine specific areas:

i. Threats, Hazards, Resilience and Contingencies, including a restricted group to consider intelligence matters;

ii. Nuclear Deterrence and Security; and

iii. Emerging Powers.

On 20 March 2011 a fourth sub-committee was established, on Libya, to co-ordinate implementation of UN Security Council Resolution 1973.

127. In addition, there are associated cross-government committees of officials that support and inform these Ministerial-level structures, headed by the Permanent Secretaries Group chaired by the National Security Adviser, Sir Peter Ricketts.[118]

128. Sir Peter was appointed National Security Adviser on 12 May 2010. When the Committee took evidence from him in October 2010, he described the operation of the new structure and its importance:

> *The Prime Minister sees the National Security Council as the forum at the heart of government that brings together foreign policy, defence policy, intelligence and homeland security [and] domestic security issues in one place, and to have systematic well-prepared meetings which bring forward the issues that need decision, particularly those that are cut across different departments and agencies*

---

[117] *www.number10.gov.uk, 12 May 2010.*

[118] *The National Security Adviser also acts as Secretary to the NSC.*

and have previously been quite hard to handle in government because there's been no one place where they all came together.[119]

129. The Heads of the intelligence and security Agencies have welcomed the new structure. The Chief of SIS told us that the NSC was *"a valuable step forward"*, and that a weekly meeting "*enabled senior Ministers to have a fuller sense of the intelligence underpinning of the issues that they are addressing*".[120] The Director of GCHQ commented that "*The quality of the debate and the exploration is first class. The chairmanship is robust but accessible*".[121] The Director General of the Security Service said that the NSC provided "*greater clarity on priorities and policy in the national security area than was available from previous arrangements*".[122]

M. The Committee welcomes the establishment of the National Security Council. It is important that there is a forum that meets regularly to enable Ministers to take decisions on national security matters and that provides an opportunity for more regular contact between Ministers and the Heads of the Agencies. The NSC must retain its current status and priority.

The National Security Strategy

130. In its 2007–2008 Annual Report[123] the ISC reported on the publication of the UK's first National Security Strategy.[124] A revised version of the strategy was subsequently published in June 2009 under the title *Security for the Next Generation*.[125] When the Committee in the last Parliament questioned the Agencies, they were told that the impact of the strategy had been limited and that it had "*little direct impact on the focus or nature of their work*".[126]

131. However, on 18 October 2010 the National Security Council published a new National Security Strategy.[127] The Strategy listed two key objectives:

i. Ensuring a secure and resilient UK – protecting the people, economy, infrastructure, territory and way of life from all major risks that can affect us directly…; and

ii. Shaping a stable world – actions beyond our borders to reduce the likelihood of risks affecting the UK or our interests overseas…[128]

---

[119] *Oral Evidence – National Security Adviser, 21 October 2010.*
[120] *Oral Evidence – SIS, 19 January 2011.*
[121] *Oral Evidence – GCHQ, 3 February 2011.*
[122] *Oral Evidence – Security Service, 9 February 2011.*
[123] *Cm 7542.*
[124] *Cm 7291.*
[125] *Cm 7590.*
[126] *Cm 7807.*
[127] *Cm 7953.*
[128] *Ibid.*

132. The Strategy also set out the 15 priority risks facing the UK, which were grouped into three 'tiers', with Tier One being the highest priority. The Tier One risks are:

- *International terrorism affecting the UK or its interests… and/or a significant increase in the levels of terrorism relating to Northern Ireland;*
- *Hostile attacks upon UK cyber space by other states and large scale cyber crime;*
- *A major accident or natural hazard which requires a national response…; and*
- *An international military crisis between states, drawing in the UK, and its allies as well as other states and non-state actors.*[129]

133. The strategy emphasised that "*all these risk areas are important*"[130] and that:

> *The inclusion of a risk in Tier Three rather than Tier Two or Tier One does not mean that it is irrelevant, or has been discounted. All of them are significant areas of concern and require government action to prevent or mitigate the risk.*[131]

However, the National Security Adviser admitted that:

> *I think it's difficult to avoid it being seen as a league table, and that all the effort goes to the top tier and no effort goes to the third tier. That would be the wrong use of it, because actually there are many risks in the third tier which are only in the third tier because a great deal of effort and money and resource is spent on keeping them in the third tier… We've played around with the naming of this. We started off by saying priority 1, 2 and 3, and a number of members of the NSC made exactly the point you are making. So we have called them Tier 1, 2 and 3, to try and reflect the fact that this is the current measure of urgency and likelihood and impact. They could change over time, and we are not saying that Tier 3 [is] unimportant.*[132]

134. The NSA did say that the "*prioritised list of risks published in the National Security Strategy [is] probably the main innovation of this document*"[133] and that while there had "*long been in Whitehall the requirements and priorities process, it has perhaps not had the status and the senior Ministerial backing*"[134] that the process now attracted as a result of the National Security Strategy. This was backed up by the Chief of SIS, who told us that the National Security Strategy is now "*the starting point for the requirements and priorities on the intelligence Agencies*".[135]

---

[129] *Ibid.*
[130] *Ibid.*
[131] *Ibid.*
[132] *Oral Evidence – National Security Adviser, 21 October 2010.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Oral Evidence – SIS, 19 January 2011.*

N. The Committee welcomes the fact that – through the National Security Strategy – the requirements process which determines the intelligence and security Agencies' allocation of effort is now given greater priority. It will be important, however, to ensure that threats lower down the hierarchy are still given appropriate attention.

The National Security Adviser

135. The National Security Adviser has three main roles:

i. to ensure that the NSC is properly served, and that it takes the right issues prepared in the right way, so that choices and options are available for Ministers;

ii. to act as personal adviser to the Prime Minister on foreign and security policy, particularly when the Prime Minister goes overseas; and

iii. to supervise the intelligence community: he has inherited from the Cabinet Secretary the role of Principal Accounting Officer[136] for the Single Intelligence Account (SIA) and also that of line manager of the Heads of the three intelligence Agencies.[137]

136. The National Security Adviser is supported by two deputies and an expanded National Security Secretariat in the Cabinet Office which has an annual budget of £49.9m.[138] The National Security Secretariat is responsible for ensuring that the Prime Minister and other senior Ministers are well supported on intelligence, security and resilience issues, and includes a strategy and counter-terrorism unit, a security and intelligence section, and an emergency planning team.

137. The NSA post effectively incorporates the roles of Head of Intelligence, Security and Resilience (in the Cabinet Office) and Prime Minister's Foreign Policy Adviser. The ISC in the last Parliament had expressed its concern at the relatively junior level of the post when the Head of Intelligence, Security and Resilience was first appointed,[139] and had continued to recommend that the post be of an appropriately senior grade. We welcome the fact that the grading of the NSA post now reflects the responsibilities of the postholder.

138. Sir Peter told us that the Agencies welcome the NSA post: they believe that it will bring about greater collaboration which will in turn bring efficiency savings. In his evidence to the Committee, he told us that:

> *I hope the Heads of the Agencies see the creation of my post as helpful to them, complementary to them, as an opportunity to co-ordinate. So many of the issues we are dealing with require the Agencies to work together, and we can facilitate that. That's our aim, not to get in their way in terms of their operational responsibilities, but to help them work together as a community.*[140]

---

[136] *The Principal Accounting Officer is responsible for assuring Parliament and the public that a high standard of probity has been exercised in the management of public funds.*

[137] *Oral Evidence – National Security Adviser, 21 October 2010.*

[138] *Of which £7.6m is for staff costs and approximately £23m is funding for BBC Monitoring.*

[139] *Cm 7299.*

[140] *Oral Evidence – National Security Adviser, 21 October 2010.*

The Joint Intelligence Committee

139. Historically the Joint Intelligence Committee (JIC) has set the Requirements and Priorities (R&Ps) for secret intelligence collection, analysis and assessment across the intelligence community.[141] However, the creation of the NSC and the tiered risks in the National Security Strategy have called into question that role (given that the latter includes a separate assessment of the priority threats facing the UK). There is now a question as to which priorities take precedence. In October 2010, the Chief of SIS stated publicly that "*we take our direction from the National Security Council*".[142] This suggests to us that the JIC R&Ps have, to some extent, been made redundant.

140. The Committee questioned the National Security Adviser on this issue. We were told:

> *There was always… this Requirements and Priorities process and table which was adopted at senior level, indeed endorsed by Ministers. Did it really provide the key template for Agency effort? I would leave a question mark. I think this is a more powerful driver… The Requirements and Priorities process… has perhaps not had the status and the senior Ministerial backing of this now prioritised list of risks published in the National Security Strategy.*[143]

141. What has become clear from our evidence sessions is that the Agencies now have a number of sets of different targets, requirements, priorities and objectives that drive their business. This has the potential for confusion. In particular, the Committee is concerned as to the value the JIC R&Ps now have in providing direction to the Agencies, and how this is consistent and aligned with the other, more recent, strategic guidance coming out of the National Security Strategy and the SDSR. It is now necessary, as a result of the changes last year, to simplify the tasking process in one place within the central machinery.

142. In January 2011, the Cabinet Secretary commissioned a review of the central security and intelligence structures to ensure that the NSC was being properly supported. The NSA and the JIC Chairman have been asked to supervise a study and provide recommendations to the Prime Minister. The review must encompass the JIC R&Ps process, which must be consistent and aligned with the NSC's requirements.

O. The Committee welcomes the creation of the National Security Adviser post, and the review of the central security and intelligence structures. As part of this review, the different sets of targets, requirements, priorities and objectives that the Agencies are subject to must be reviewed and simplified: there must be one clear tasking process. In particular, it is important that the work of the Joint Intelligence Committee, and the Requirements and Priorities process, is aligned with the strategic direction being set by the National Security Council.

---

[141] *The R&Ps are based on a matrix which ranks geographic and organisational targets against strategic themes and threats.*

[142] *Speech to the Society of Editors, 28 October 2010.*

[143] *Oral Evidence – National Security Adviser, 21 October 2010.*

The Strategic Defence and Security Review

143. On 19 October 2010, the Government published its Strategic Defence and Security Review (SDSR).[144] Although the SDSR was predominantly about defence equipment, structures and capabilities, it also provided guidance on priorities for intelligence activity, noting that:

> *Our adaptable approach to national security will require that our intelligence capabilities continue to support our core military, diplomatic, security and domestic resilience requirements and our economic prosperity.*[145]

144. The SDSR also identified eight key cross-departmental 'National Security Tasks':

i. *Identify and monitor national security risks and opportunities;*

ii. *Tackle at the root the causes of instability;*

iii. *Exert influence to exploit opportunities and manage risks;*

iv. *Enforce domestic law and strengthen international norms to help tackle those who threaten the UK and our interests;*

v. *Protect the UK and our interests at home, at our border and internationally, to address physical and electronic threats from state and non-state sources;*

vi. *Help resolve conflicts and contribute to stability. Where necessary, intervene overseas, including the legal use of coercive force in support of the UK's vital interests, and to protect our overseas territories and people;*

vii. *Provide resilience for the UK by being prepared for all kinds of emergencies, able to recover from shocks and to maintain essential services; and*

viii. *Work in alliances and partnerships wherever possible to generate stronger responses.*

These tasks are high-level and do not contain specific detail to guide the work of the Agencies and Armed Forces: the SDSR recognised that "*we need to maintain flexible capabilities to respond to changing pressures and priorities*".[146]

145. In line with the priority afforded to the cyber threat in the National Security Strategy, the SDSR announced that £650m of 'new' funding would be made available for cyber security.[147]

---

[144] *Cm 7948.*

[145] *Ibid.*

[146] *Ibid.*

[147] *Further details can be found in paragraphs 186 to 207.*

Counter-Terrorism responsibilities and reviews

The Office for Security and Counter-Terrorism

146. The Office for Security and Counter-Terrorism (OSCT) was established within the Home Office in March 2007. It was created to enable the Home Office to take responsibility for setting the strategic direction for, and co-ordination of, the Government's Counter-Terrorism Strategy, CONTEST (which had previously been within the Cabinet Office's remit).

147. OSCT's main responsibilities are to:

- *support the Home Secretary and other Ministers in directing and implementing CONTEST;*
- *deliver aspects of this strategy directly, through legislation, guidance and funding;*
- *set the strategic government response to terrorism-related crises through the Cabinet Office Briefing Room (COBR) mechanism;*
- *manage the Home Secretary's statutory relationship with the Security Service; and*
- *manage the Olympic and Paralympic safety and security programme for the London 2012 games.*[148]

Expansion of OSCT

148. OSCT has continued to grow since 2007. In its 2008–2009 Annual Report the ISC noted that:

> *This expansion [of OSCT] has resulted in an increase in staff from 270 in 2007 to 320 permanent staff as at January 2009.*[149]

This year, the Committee was told there are now around 400 staff working in OSCT.[150] This means that OSCT has increased by around 50% since it was created just four years ago.

149. The Committee in the last Parliament questioned the then Home Secretary on the need for so many people in strategy and co-ordination roles,[151] and whether these resources could be better used to fund front-line positions. The expansion, in 2010, of the National Security Secretariat in the Cabinet Office – which also co-ordinates and develops strategy in relation to national security issues, and which now includes its own Counter-Terrorism strategy team – increases such concerns.

---

[148] *www.homeoffice.gov.uk/counter-terrorism/OSCT*

[149] *Cm 7807.*

[150] *Oral Evidence – Home Secretary, 24 November 2010.*

[151] *Oral Evidence – Home Secretary, 28 April 2009.*

P. The Committee remains concerned about the overlap in remit and potential for duplication of work between the Office for Security and Counter-Terrorism and the National Security Secretariat in the Cabinet Office. Since central structures are currently being examined, we recommend that thought is given to OSCT's future role in the light of that review.

Review of the Counter-Terrorism Strategy (CONTEST)

150. While the National Security Strategy sets the strategy across the wide range of security issues, CONTEST focuses specifically on Counter-Terrorism. The stated aim of CONTEST is:

> *To reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence.*[152]

151. CONTEST covers four distinct areas:

i. Pursue: *to stop terrorist attacks;*

ii. Prevent: *to stop people becoming terrorists or supporting violent extremism;*

iii. Protect: *to strengthen our protection against terrorist attack; and*

iv. Prepare: *where an attack cannot be stopped, to mitigate its impact.*[153]

152. In July 2010, the Home Office announced that CONTEST would be revised, to align it with the 2010 Spending Review and the Strategic Defence and Security Review.[154] Work began in November 2010 and was due to be completed by the end of January 2011. The publication has, however, been delayed in order to allow the prior publication of the PREVENT Review and Strategy, and the 7/7 Inquest report. The strategy had not been published in time to be considered as part of this Annual Report.

Review of the PREVENT strand of CONTEST

153. In June 2010, the Home Office had already begun separately to review the PREVENT strand of CONTEST.[155] The SDSR described the purpose of this review as:

> *Separating [PREVENT] much more clearly than before from general communities policy. The Department for Communities and Local Government will work to encourage a more integrated society, separate from CONTEST, while the Office for Security and Counter-Terrorism… will be responsible for a more focussed Prevent Strategy.*[156]

---

[152] *Cm 7547.*

[153] *Ibid.*

[154] *Home Office Structural Reform Plan, published on Number 10 website, July 2010.*

[155] *Ibid.*

[156] *Cm 7948.*

154. In evidence to the Committee about the PREVENT review, the Home Secretary said:

> *One of the concerns I have had about… the past is that we have ended up with… work taking place which is sullied in some people's eyes by the Counter-Terrorism message because it is seen to be purely about Counter-Terrorism. 'You are only talking to us, you are [only] trying to do something because you want to stop us blowing you up' is the sort of message… I think there's a lot the Government can do in working with Muslim communities and talking to them about issues that matter to them, that are nothing whatsoever to do with Counter-Terrorism, that gives a clear message that actually Government perceives them as part of British society and doesn't see them as a group that has to be treated in some sort of different way, purely because they happen to be from a particular community.*[157]

155. Whilst this separation is important, it is equally important that any revised PREVENT strategy has clear indicators of success. The ISC in the last Parliament expressed concern regarding the lack of such indicators to measure the impact of PREVENT (into which Agency and police resources have been allocated over the past few years). In its 2008–2009 Annual Report the ISC said that:

> *Given the importance of this work, and the considerable funding it is receiving, it is essential that clear and transparent targets are in place against which progress can be measured… [We] recommend that more effective measures are developed against which to assess progress.*[158]

156. The difficulty of measuring the success of PREVENT work is most notable in the work of the Research, Information and Communications Unit (RICU), which was established in 2007 with the primary aim of ensuring consistency, across government, on Counter-Terrorism and counter-extremism messages and developing a coherent narrative to challenge extremist ideology. RICU is jointly funded by the Home Office and the Foreign Office. It currently has 22 full-time staff and its budget in 2010/11 was £4.25m (of which £0.3m was spent on research and £2.7m was spent on communication campaigns).

157. The two most high-profile campaigns run by RICU in 2010/11 were:

- UK Counter-Narrative Campaign, described as "*a project to establish a loose network of credible community groups able to directly challenge terrorist propaganda*";[159] and
- Victims' Testimonies – International, described as "*a project to help a [non-governmental organisation] representing victims of terrorism to counter terrorist propaganda by amplifying victims' voices in territories most exposed to terrorist propaganda*".[160]

---

[157] *Oral Evidence – Home Secretary, 24 November 2010.*

[158] *Cm 7807.*

[159] *Briefing provided by the Home Office, 19 May 2011.*

[160] *Ibid.*

RICU also ran a number of research campaigns, of which the most high-profile was research on 'threat communications', which aimed "*to understand better how the public receives and understands the threat level from international terrorism*".[161]

158. RICU has now been in existence for four years. The Committee in the last Parliament was critical of the practical benefits it has been able to demonstrate. In its 2008–2009 Annual Report it said:

> *... this is a difficult area of work where progress takes time, and is hard to see and measure. We hope that the results will be visible in the future, but note that RICU itself has said that 'communications can only take us so far'.*[162]

159. The Committee discussed this issue with the Home Secretary this year. The Director General of OSCT said:

> *How do we measure impact? Using techniques that we have been introduced to by communications experts, reading material that we have supported. What influence does that material have? How credible do they find that material? And ultimately, of course, to what extent does it make an impact on either their behaviours or indeed outlooks, thinking… I think the metrics for communications work are relatively well established. I'm certainly not saying they are perfect, but it's not a new machine for many people working in the communications industry.*[163]

160. The Home Secretary agreed, however, that it was a complex issue:

> *We are looking at the work that RICU does, and looking more generally at the issues across the PREVENT work and RICU work… I think one of the challenges… is identifying how we can measure the impact the PREVENT work has had. That's one of the challenges we are grappling with.*[164]

Q. The Committee accepts that it is not easily achieved, but it is nevertheless essential that there is some mechanism by which the success of work on the PREVENT strand of CONTEST – and the benefits of RICU in particular – can be evaluated.

161. Like the CONTEST review, the review of PREVENT was originally intended to be completed by January 2011. However, it was not published until 7 June 2011. This proved too late to review as part of this Annual Report.

---

[161] *Ibid*

[162] *Cm 7807.*

[163] *Oral Evidence – Home Secretary, 24 November 2010.*

[164] *Ibid.*

Review of Counter-Terrorism powers

162. In July 2010, the Home Secretary also announced a "*rapid review of key Counter-Terrorism and security powers*".[165] Although originally due to report in autumn 2010, it finally reported on 26 January 2011.[166]

163. This Committee is primarily concerned with the impact of the review on the intelligence and security Agencies and we have therefore focused on the changes to the Control Orders regime. The review concluded that the existing legislation governing Control Orders[167] should be repealed and replaced with "*a less intrusive and more focused regime*" – Terrorism Prevention and Investigation Measures.[168] Specifically, the changes proposed include:

- the abolition of forced relocation (although exclusion measures will still exist);
- a replacement of (up to) 16 hour curfews with an overnight residence requirement;
- more limited restrictions on telephone and internet usage; and
- a reduction in the banning of associations.[169]

The changes will not be implemented immediately and the existing legislation was renewed until 31 December 2011 in order to allow the Government time to introduce new legislation.

164. We questioned the Director General of the Security Service as to whether the new regime would enable the Service to provide the same level of assurance as they had been able to with Control Orders. The Director General told us the Service had advised the Home Secretary that:

> *Control Orders have assisted us in managing the threat from terrorism, and that removing or significantly weakening them would reduce the level of assurance that we are able to provide within our existing resources… Covert investigation does not deliver disruption and therefore cannot replicate the effect of the current system of Control Orders.*[170]

He told the Committee that "*I am… confident that all decisions were made with a full understanding of the threat*".[171]

165. The Committee is concerned that the new regime does not offer the same level of assurance. We are also concerned at the impact that the changes will have on the Service, as a result of the increased pressure on resources, both in terms of surveillance and other covert investigative tools available to them. The Committee is aware from its reports

---

[165] *www.homeoffice.gov.uk/media-centre/press-releases/counter-powers/*

[166] *www.homeoffice.gov.uk/publications/counter-terrorism/review-of-ct-security-powers/*

[167] *The Prevention of Terrorism Act 2005.*

[168] *Cm 8004.*

[169] *Terrorism Prevention and Investigation Measures Bill (as introduced), HC Bill 193, 23 May 2011.*

[170] *Written evidence – Director General, Security Service, 27 January 2011.*

[171] *Ibid.*

on the 7 July 2005 London bombings that surveillance, in particular, is highly resource-intensive and places a significant burden on the Security Service.

166. We note that in evidence to the Joint Committee on Human Rights, the then Security Minister, Baroness Neville-Jones, said that a transitional period was necessary to ensure that the Security Service and police had sufficient resources to provide the extra surveillance and associated investigatory capacity and that "*the resources that the… Security Service have open to them at the moment do not stretch to this*".[172] The Committee therefore questioned the Director General as to whether the Service had the capacity to carry out surveillance on greater numbers of individuals and if that would have an impact on the resources currently allocated to operations. We were told that, in recognition of the increased burden, the Security Service would be receiving additional funds of £***m in the first year, rising to £***m per year thereafter, in order to supplement their investigative capacity – of which physical surveillance is only one element.[173]

167. The Committee further questioned the Director General as to whether – even with the additional resources – this policy would have an adverse impact on the Service's ability to cover lower-priority (but nonetheless important) targets. He said:

> *… this is not an area which lends itself to precision, and levels of assurance relate not solely to specific cases but to the broad threat picture and the calls on investigative capacity at any one time. We anticipate that our ability to cover lower-priority [targets]… will be largely unchanged… I was not asked to undertake to deliver the same level of assurance once Control Order legislation has been repealed but I am content that as a result of the replacement legislation and the additional funding that has been made available, there should be no substantial increase in overall risk.*[174]

R. The Committee notes the assurance provided by the Director General of the Security Service that, with additional funding and the measures included in the Terrorism Prevention and Investigation Measures Bill, there should be no substantial increase in overall risk. However, any increase at all in the overall threat to national security would be a matter of serious concern. The Committee will take further evidence on the impact of the new regime in due course.

S. Counter-Terrorism work must be effectively co-ordinated and there must be a clear strategy. Work falling under CONTEST has been subject to a number of separate reviews over the last year. The Government must ensure that these do not operate in isolation from each other and that the end result is properly co-ordinated.

Defence Intelligence

168. Defence Intelligence (DI) is part of the Ministry of Defence (MoD) and funded through the main MoD budget. DI provides strategic intelligence to inform MoD policy and procurement decisions and to support military operations overseas.

---

[172] *HC 838, 2 March 2011.*

[173] *Written evidence – Security Service, 27 January 2011.*

[174] *Written evidence – Security Service, 21 February 2011.*

Strategic priorities

169. Prior to 2009, DI's strategic priorities were set out in the Requirements and Priorities for Defence Intelligence (RPDIs), which were consistent with the Requirements and Priorities (R&Ps) produced by the Joint Intelligence Committee (JIC) but included additional specific requirements in support of defence objectives. DI subsequently reduced its reliance on JIC R&Ps and instead the Chief of Defence Intelligence's (CDI's) priorities were set out in a Strategic Tasking Directive by the Chief of the Defence Staff and the Permanent Under Secretary[175] at the MoD.

170. In March 2009, CDI told the Committee in the last Parliament that this change from the RPDIs to the Strategic Tasking Directive:

> *… allowed more flexibility to move between priorities… There will be some differences… [because] the JIC R&P is looking at some areas that are not core areas of interest for MoD… My tasking directive allows me to take those differences into account in setting the work we undertake.*[176]

171. However, the first Strategic Tasking Directive – which was set for 2008/09 – has not been updated since. When the Committee questioned CDI on the reasons for this, he explained that the 2008/09 document was still relevant, and the main reason that it had not been revised was because DI had now taken "*a deliberate decision… to take a slightly different tack*" and to "*try and work more formally through the JIC R&P process*".[177] He said:

> *… although I think that broadly [the Strategic Tasking Directive] achieved its aim, what it didn't achieve was ensuring that we are absolutely aligned… with the national priorities…*[178]

T. It is disappointing that the Strategic Tasking Directive did not prove a satisfactory system for setting Defence Intelligence's priorities. In devising a new process, Defence Intelligence must take account of the results of the review of central intelligence structures and strategies, and the implications of that review for the setting of national priorities and tasking of the intelligence community.

Support to military operations

172. Notwithstanding the process through which the strategic priorities are identified, DI's main focus is, and always has been, support to current military operations. During 2009/10 DI continued its vital work in support of the campaign in Afghanistan.

173. A key development during 2009/10 was the creation of the Defence Intelligence Fusion Centre (Afghanistan) (DIFC(A)), which became fully operational in June 2010. The purpose of DIFC(A) is to draw together DI's all-source analysis on Afghanistan

---

[175] *The most senior civil servant at the Ministry of Defence.*

[176] *Oral Evidence – CDI, 3 March 2009.*

[177] *Oral Evidence – CDI, 17 March 2011.*

[178] *Ibid.*

regionally into one team: DI told us that over ***% of the DI Assessments staff were now working in DIFC(A).[179] The Committee questioned CDI about the practical benefits of DIFC(A) and we were told:

> *[It] bring[s] together a whole range of different… expertise… we have brought together our joint UK/US team which looks at the narcotics threat… our teams which look at the Improvised Explosive Device threat… our team which looks at social networks… together with those who are providing the strategic perspective of the military insurgency and the political situation, both in Afghanistan and Pakistan. And by bringing them all together, both organisationally and physically, we are getting a much better answer out.*[180]

HUMINT capability and Improvised Explosive Devices (IEDs)

174. The Defence Human-sourced Intelligence (HUMINT) Unit is a critical part of DI's intelligence collection capability. In his Annual Update to the Committee, CDI said:

> *Human intelligence on [counter]-IED reporting continues to enhance force protection in theatre and, in the majority of circumstances, HUMINT threat warnings trigger imagery intelligence analysis.*[181]

Therefore DI's HUMINT capability is particularly vital to its efforts to counter the threat to our Armed Forces from IEDs, which remains a top priority.

175. In the past, the ISC has expressed concern about the strength of DI's HUMINT capability. In its 2008–2009 Annual Report the Committee said:

> *CDI told us that in both Iraq and Afghanistan the value of HUMINT 'has perhaps been much greater than we have seen in previous operations'. We were therefore concerned to be told that:*
>
> > *[Although] Defence HUMINT assets continue to be heavily engaged in current operations with some notable successes… the ability of the Unit to support these operations and a range of additional commitments… remains fragile.*[182]

176. The Committee was therefore reassured to be told that DI had received approval in 2009 for additional staff to expand its HUMINT capability, ***. We were, however, surprised, this year, to be told that only approximately 25% of these would be in post by the end of 2011, and we questioned CDI as to why this process could not be accelerated.[183] We were told:

> *… in the case of advanced HUMINT operators, they have to go on a very long course. And we are getting about a 50 or 60% pass rate on that… I am resource constrained on… the number of instructors that I have available… but we get*

---

[179] *Written Evidence – Defence Intelligence, 15 April 2011.*

[180] *Oral Evidence – CDI, 17 March 2011.*

[181] *Written Evidence – Defence Intelligence, 18 December 2010.*

[182] *Cm 7807.*

[183] *Oral Evidence – CDI, 17 March 2011.*

around that by taking guys and girls who have come back from the theatre, who are highly experienced, and we employ them as instructors in their downtime.[184]

177. The Committee asked CDI whether the shortage of HUMINT resources was having an impact on their ability to detect IEDs and therefore protect our forces. We were told:

… the simple answer, of course, is that we have resourced Afghanistan at the cost to our people. So we haven't reduced the number of teams we have in Afghanistan. They are just turning around quicker and having to go back more often.[185]

U. The Committee welcomes the fact that Defence Intelligence is recruiting additional staff to expand its HUMINT capability, which is vital to counter the threat to our Armed Forces from Improvised Explosive Devices in particular. However, the Committee is concerned that the shortage of HUMINT instructors means that these new recruits cannot be deployed quickly. It is also concerning that existing HUMINT operators, who were already under pressure covering vacancies in theatre, are now being placed under further pressure by having to train the new recruits.

Other areas of work

178. In addition to its core work supporting military operations, other key areas of activity for DI during 2009/10 included:

- work on Iran (***);
- ***;
- assessments on Chemical, Biological, Radiological and Nuclear (CBRN) threats to the UK and UK interests overseas;
- continued assessment on Russia (including current and future intent and capabilities, Russian National Security Strategy, military doctrine and armed forces reforms, studies on the economy and defence budget ***);
- provision of technical support and advice on technology proliferation issues to international export control regimes; and
- maintaining the unique and valuable capability provided by ***.[186]

Staffing reductions

179. During 2008/09, staff in MoD headquarters were reduced by 20%. This resulted in the loss of 122 posts in DI, of which just under half were analytical staff. The ISC in the last Parliament was critical about these reductions because they had been told that there were already insufficient resources to meet the requirements of DI customers: at the time CDI said, "*in some areas we are still covering the area but with fewer people and in other areas we have had to drop outputs completely*".[187] In its 2008–2009 Annual Report, the Committee commented:

---

[184] *Ibid.*

[185] *Ibid.*

[186] *Written Evidence – Defence Intelligence, 18 December 2010.*

[187] *Oral Evidence – CDI, 3 March 2009.*

[We remain] concerned that these reductions in [DI] staff numbers will have a serious impact on [DI's] capability. They could also have long-term implications for [DI] core customers and the wider intelligence community.[188]

180. Under the 2010 Spending Review, the MoD as a whole is facing real-terms cuts of 8% between now and 2015. This will inevitably mean further cuts for DI. We therefore questioned CDI about the impact this will have on DI's capability. He said:

... no decisions have been made... It will involve difficult decision[s] because there are no... whole areas that we could just get rid of, without impacting on the total intelligence picture... I think it would be realistic to assume that we will have to take a share of MoD's reductions... If you delete a capability completely, regenerating it could take 10, 15, 20 years.[189]

181. This is even more concerning given that DI is heavily reliant on BBC Monitoring which is itself facing stringent cuts under the 2010 Spending Review, as we describe at paragraphs 245 to 255. When we asked CDI about the importance of BBC Monitoring to DI, he said:

Open source is... increasingly important to us; partly because it is growing and partly because our capabilities are reducing.[190]

182. It is difficult to envisage how DI will be able to maintain adequate coverage if reductions in both organisations are made.

V. Defence Intelligence provides the largest single all-source assessment capability within the UK intelligence community. The ISC has, since 2008, consistently raised concerns about the diminution of its coverage and capability. The prospect of further cuts – combined with the impact of cuts to BBC Monitoring, on which DI relies heavily – therefore has potentially very serious long-term consequences for DI's ability to support military operations and for the UK intelligence community as a whole.

Modernisation Programme

183. DI has been running a Modernisation Programme for some years. One of the major projects within this programme is the relocation of various elements of DI's intelligence collection capabilities at a new facility at RAF Wyton. Construction of the new site, known as the Defence Geospatial Intelligence Fusion Centre, was due to commence in late 2008 and take two years. However, a number of delays ensued and in June 2010, CDI wrote to the Committee to say that the centre would not be up and running until August 2013.

---

[188] *Cm 7807.*

[189] *Oral Evidence – CDI, 17 March 2011.*

[190] *Ibid.*

184. The Committee questioned CDI about the delay to this project. We were told that:

> *The original delay was due to the fact it took us longer to get the approvals… with the Treasury than we had thought. [A further delay of one year was caused] because of MoD funding problems, we had to have some money removed… that money was fed back in the following year.*[191]

185. The Committee asked whether this had led to increased costs. We were told, "*[Yes] that increased the costs… but that was no problem to the programme because we were given… extra funding to do that.*"[192]

[191] *Ibid.*

[192] *Ibid.*

SECTION 6: CROSS-CUTTING ISSUES

Cyber security

The threat

186. Businesses and individuals are increasingly dependent on cyber space, from the use of email and other communication methods to internet shopping: an Office for National Statistics survey in August 2010 indicated that over 30 million adults use the internet every day. However, in doing so they are exposed to risks. In its 2008–2009 Annual Report the ISC raised concerns about the potential threat posed to the UK Government, Critical National Infrastructure and commercial companies from electronic attack and recommended that the UK accord cyber security a higher priority.[193]

187. In June 2009 the Cabinet Office published the *Cyber Security Strategy of the United Kingdom*[194] which stated that cyber security is "*an urgent and high-level problem which cannot be ignored*". In January 2010 the Chief of SIS told the Committee that "*the whole question of cyber security is shooting up everybody's agendas*".[195] Then, in October 2010 the National Security Strategy listed "*Hostile attacks upon UK cyber space by other states and large scale cyber crime*"[196] as a Tier One risk, explaining that:

> *Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals… unless we take action, this threat could become even worse. For this reason, cyber security has been assessed as one of the highest priority national security risks to the UK.*[197]

188. Hostile attacks upon UK cyber space can be launched by individuals (such as hackers), non-state actors and groups such as criminals and terrorists, or by governments. The threat can be broken down into crime, espionage and terrorism:

> *(i) Crime*
>
> The primary threat to cyber security comes from crime.[198] According to NATO, 90% of computer penetration is with criminal (primarily fraud), rather than political or strategic, intent.[199] Most of the software and knowledge required to commit cyber crimes is now readily available from criminal websites and discussion boards. However, countermeasures are similarly easily accessible. The Serious Organised Crime Agency (SOCA) assesses that up to 80% of online fraud could be prevented if individual internet users observed basic security practices such as keeping their security and anti-virus software up to date, and choosing better passwords.[200]

---

193 *Cm 7807.*

194 *Cm 7642.*

195 *Oral Evidence – SIS, 19 January 2010.*

196 *Cm 7953.*

197 *Ibid.*

198 *The cost of cyber crime to the UK is estimated at £27bn a year according to 'The Cost of Cyber Crime', Detica report for Cabinet Office, February 2011.*

199 *Cyber Security: A Transatlantic Perspective, Security and Defence Agenda, March 2010.*

200 *Sir Ian Andrews, Chair of SOCA, Cyber Security Summit, 9 November 2010.*

(ii) Hostile Foreign Activity

Cyber space means that countries no longer have to invest in global networks and pursue complex operations with high-level agents when it comes to espionage: they can access much of the same information using relatively inexpensive cyber attacks. The Director General of the Security Service told us in February 2011 that "*the barriers to entry to cyber espionage are quite low. We have found a number of… countries taking an interest in this*".[201] GCHQ elaborated on the source of the threat:

> *The greatest threat of electronic attack continues to be posed by State actors and, of those, Russia and China are [suspected of carrying out] the majority of attacks. ***. Their targets are in Government as well as in industry. ***. There are also a number of other states with credible electronic attack capabilities ***.*[202]

Currently the main purpose of such attacks is espionage and the acquisition of information; however, there is a concern that this capability could be turned towards disruption activities – for example, interrupting supply of utility services:

> *The capability [that states] use for espionage purposes could be used to do other things if they needed to. So where they are positioned to get espionage, that in itself is a threat that they could cause disruption, whether they are doing disruption now or not.*[203]

(iii) Terrorism

The internet is an ideal environment for ideological and political extremists and has been described as a "*virtual extremist madrassa*".[204] The Dutch Intelligence Service has described the internet as the "*turbocharger of radicalization*",[205] since it offers a means of disseminating extremist propaganda and technical knowledge efficiently. However, we have been told that "*terrorist groups currently tend to limit online activity to communication tools and virtual meeting places*".[206] ***.[207]

The response

189. The Strategic Defence and Security Review (SDSR) announced in October 2010 that £650m of 'new' funding would be made available across government for a "*transformative national cyber security programme* (NCSP)".[208] This programme will:

- overhaul the UK's approach to tackling cyber crime;
- address deficiencies in the UK's ability to detect and defend against cyber attack;

---

[201] *Oral Evidence – Security Service, 9 February 2011.*

[202] *'Update on the Nature of the Threat Posed by Electronic Attack', Briefing provided by GCHQ, September 2010.*

[203] *Oral Evidence – Security Minister, 13 January 2011.*

[204] *Senate Committee on Homeland Security, 'Violent Islamic Extremism, the Internet, and the Homegrown Terrorist Threat', May 2008.*

[205] *'World Wide Web of Terror', The Economist, 14 July 2007.*

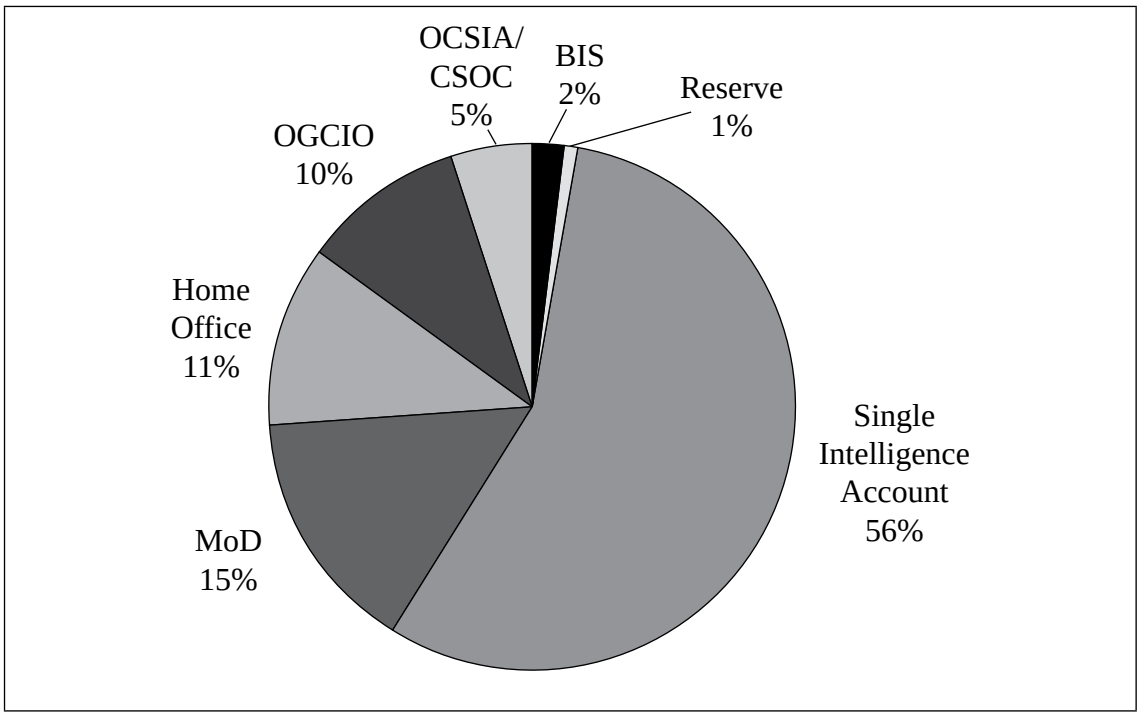
[206] *'The Nature and Scale of the Cyber Threat to the UK', Briefing provided by OCSIA, December 2010.*

[207] *Ibid.*

[208] *Cm 7948.*

- address shortcomings in the UK's critical cyber infrastructure;
- sponsor long-term cyber security research; and
- introduce a new programme of cyber security education and skills.[209]

190. The Committee has been informed[210] that of the £650m of 'new' money, £50m is coming from within the Single Intelligence Account settlement. The remaining £600m (which is new money) is to be spent over a four-year period and will be divided up in the following way:



Responsibilities and co-ordination

191. There are 18 departments, units or agencies with particular responsibilities for aspects of cyber security. These are spread across the intelligence and security Agencies, law enforcement, and other government departments including the Home and Foreign Offices, MoD and the Department for Business, Innovation and Skills (BIS). The teams cover a range of functions including formulating policy, managing the response across government and conducting operational activity:

[209] *Briefing provided by the Office of Cyber Security, December 2010.*
[210] *Ibid.*

Department/ Agency	Unit	Core functions
Cabinet Office	Office of Cyber Security and Information Assurance (OCSIA)	Policy/ Management
	Cyber Security Operations Centre (CSOC) which is hosted by GCHQ	Analysis/Incident Response
	Office of the Government Chief Information Officer (OGCIO)	Policy
GCHQ	Communications-Electronics Security Group (CESG)	Protection/ Incident Response
	Network Defence Intelligence and Security Team (NDIST)	Analysis
	Internet Operations Centre (INOC)	Operations
Security Service	Cyber Investigations Team	Operations
SIS	Works overseas in support of, primarily, GCHQ operations	Operations
	Technical and Information Security Team	Protection
Home Office	Crime and Policing Group	Policy/ Management
Serious Organised Crime Agency	E-Crime Department	Operations
Police	Police Central e-Crime Unit (PCeU) hosted by the Metropolitan Police	Operations/Policy
	Child Exploitation and Online Protection Centre	
Ministry of Defence	Defence Cyber Operations Group	Protection
	Defence Science and Technology Laboratory (DSTL)	Operations
BIS	Cyber Infrastructure Team	Policy
Foreign Office	FCO's global network supports HMG's cyber security agenda	Policy/ International liaison
Other	Centre for the Protection of National Infrastructure (CPNI)	Protection/ Analysis

192. While there are a number of departments involved in cyber security, the work is led by the Cabinet Office.

(i) Office of Cyber Security and Information Assurance (OCSIA)

The Office of Cyber Security (OCS) was first established in the Cabinet Office in June 2009 following publication of the Cyber Security Strategy. In September 2010 it expanded to become the Office of Cyber Security and Information Assurance (OCSIA) with the aim of "*providing a joined-up and coherent strategic and policy lead for cyber security and Information Assurance across government*".[211] OCSIA is based in the National Security Secretariat under Sir Peter Ricketts, and has 27 staff mostly recruited from across government with a small number from the private sector.

(ii) Cyber Security Operations Centre (CSOC)

CSOC (established in 2009) is hosted by GCHQ; however, it is the Director of OCSIA in the Cabinet Office who provides the 'operational direction'.[212] CSOC produces reports and assessments on cyber security issues affecting the UK, and provides cyber security incident management and co-ordination. CSOC currently has 19 staff drawn from a wide range departments, but plans to increase this to 30 during 2011.

193. Initially, however, Ministerial responsibility lay in a third department – the Home Office – under the Minister for Security.[213] This division between Minister and officials (the latter being themselves split between GCHQ and the Cabinet Office) was far from ideal. The Committee asked Baroness Neville-Jones about the structures and she conceded that "*you are pointing to a formal loophole in the system, and I don't argue with you that that may exist*".[214]

194. The Committee's concern at this potential for confusion (and for duplication) was reinforced in evidence given by the Agencies. The Director General of the Security Service told us that "*it's not absolutely clear what the overall architecture is going to be for cyber security*".[215] Meanwhile, the Chief of SIS told the Committee that "*I'm not sure the Cabinet Office processes for determining what is a coherent cyber programme [are] as sophisticated as [they] should be*".[216]

195. On 17 May 2011, Ministerial responsibility for cyber security transferred to the Minister for the Cabinet Office.

---

[211] *Briefing provided by OSCIA, December 2010.*

[212] *Ibid.*

[213] *Baroness Neville-Jones was Minister for Security and Counter-terrorism, with responsibility for cyber security, from 13 May 2010 to 9 May 2011.*

[214] *Oral Evidence – Security Minister, 13 January 2011.*

[215] *Oral Evidence – Security Service, 9 February 2011.*

[216] *Oral Evidence – SIS, 19 January 2011.*

W. The Committee welcomes the identification of cyber security as a Tier One risk in the National Security Strategy and the increased investment in this crucial area. However, concerns expressed in the ISC's last Annual Report concerning the lack of clear lines of responsibility and the potential risk of duplication of effort remain. The interests of national security demand that there should be clear lines of Ministerial accountability. We expressed concern that the original system was neither sensible nor appropriate. We strongly support the Government's decision to move Ministerial responsibility to the Cabinet Office.

The Agencies' response

196. The intelligence and security Agencies have a key role to play in tackling the cyber threat to the UK and have established teams to take forward their particular responsibilities.

GCHQ

197. Baroness Neville-Jones told us that, with regard to cyber security, "*GCHQ, which is the national technical agency… is where, in a sense, the crown jewel lies in capability*".[217] At present, GCHQ has over *** staff directly engaged in cyber security-related work. However, GCHQ has stressed that "*Cyber is also a fundamental, inextricable part of much of the work of GCHQ as a whole and thus it is difficult to quantify exactly*".[218]

198. GCHQ's work in relation to cyber security includes the following four categories:

(i) Protection: Communications-Electronics Security Group (CESG)

As explained above in paragraph 58, CESG is the national technical authority for Information Assurance (IA).

(ii) Analysis: Network Defence Intelligence and Security Team (NDIST)

NDIST is responsible for the investigation and analysis of electronic attack activity which has the potential to damage UK strategic interests.

(iii) Intelligence-gathering: Internet Operations Centre (INOC)

The INOC, which was established in 2007, brings together all of GCHQ's computer network operations capability in one team in support of internet-related operations.

(iv) Military Capability

When hostile actors use the internet or cyber attack methods, they too become vulnerable. GCHQ has informed the Committee that it is "*working with MOD and the Defence Science and Technology Laboratory to develop [a military] Cyber capability for the UK*" and that some of this will involve the development and testing of new technical capability.[219]

---

[217] *Oral Evidence – Security Minister, Cyber Security, 13 January 2011.*

[218] *Written Evidence – GCHQ, 14 December 2010.*

[219] *Ibid.*

199. GCHQ has been provisionally allocated *** for the National Cyber Security Programme. It is also reallocating £50m of its own budget to cyber work. The Director told us that this money would be spent in several ways:

> *We will improve our view of hostile activity on the internet, so that is ensuring that as much as possible of our internet access will be capable of detecting electronic attacks coming in… ***… We will try and come up with better analytical tools to detect, understand and attribute attacks. There will be some research into [military] cyber capabilities… [and] protecting our own systems from infection.*[220]

SIS

200. SIS describes its cyber work as "*distinctive*" because its agent reporting is "*an enabler of critical parts of GCHQ's cyber detection and defence work and as a future enabler of* ***".[221] Specifically, SIS's contribution to the work of GCHQ includes:

i. ***;

ii. using SIS's global network *** to provide information to GCHQ;

iii. ***; and

iv. a joint SIS–GCHQ team which acquires *** intelligence about specific parts of ***.

201. SIS is set to receive approximately *** of the total SDSR cyber money. With this funding SIS will provide more intelligence to support GCHQ's operations and coverage ***.[222]

202. However, SIS told the Committee that the money it received was less than it had bid for, and that this will have an impact on its ability to deliver against all these areas. The Chief said: "*When we apply ourselves to targets, we produce the goods. But if we don't have the resources to apply ourselves to the targets, we produce fewer goods.*"[223]

Security Service

203. The Security Service employs cyber techniques across the full range of its work ***.[224]

204. The Service is integrating digital intelligence into all of its investigations. In 2009 the Service established a Digital Intelligence (DIGINT) Programme with the aim of allocating more staff and improved technology to digital intelligence gathering and analysis, and devoting more resources to technological research and development. One of the first goals of the programme was the allocation of dedicated digital intelligence analysts to all investigative teams.

---

[220] *Oral Evidence – GCHQ, 3 February 2011.*

[221] *Written Evidence – SIS, 14 December 2010.*

[222] ***.

[223] *Oral Evidence – SIS, 19 January 2011.*

[224] *Written Evidence – Security Service, 14 December 2010.*

205. Building on the foundations of its DIGINT Programme, the Service is now focused on establishing and implementing a programme which will deliver a stronger capability to investigate specifically the threat from hostile foreign actors engaged in cyber espionage against the UK. The Service has already created a joint team of technical cyber security experts and counter-espionage investigators. Building on the existing expertise gained from investigation of other types of espionage and working collaboratively with the other Agencies, this will enable the Service to make a more substantial investigative/operational contribution to UK cyber security and improve the flow of relevant threat information to the private sector.

206. In conjunction with the Security Service, responsibility for engaging the private sector on cyber security rests with the Centre for the Protection of National Infrastructure (CPNI), which gives advice on protective security to owners of Critical National Infrastructure in government and the private sector. CPNI advice aims to reduce the vulnerability of key physical, personnel and information assets to attack, primarily from terrorism, but also from Hostile Foreign Activity. Its work covers physical security (e.g. access controls and protecting against bombs), electronic security (e.g. cyber attack or electromagnetic pulse devices) and personnel security (e.g. staff vetting). In the coming years the provision of cyber security advice to a growing range of private sector organisations, within and beyond the UK's Critical National Infrastructure, is likely to be the principal growth area for CPNI. This is consistent with the importance that CPNI has placed on information security since its creation.

207. The Security Service has been allocated *** from the additional cyber funding. The Service has informed the Committee that its priorities for this money will be to support the investigative and advisory roles outlined above.[225]

Detainees

208. The role of the UK intelligence and security Agencies in relation to detainees in the custody of foreign powers has been the subject of considerable debate, speculation, allegations and legal action over the last decade.[226] In an attempt to draw a line under these problems, on 6 July 2010 the Prime Minister announced a package of measures relating to the UK's involvement with detainees. He told the House of Commons:

> *For the past few years, the reputation of our security services has been overshadowed by allegations about their involvement in the treatment of detainees held by other countries… Those allegations are not proven… Our reputation as a country that believes in human rights, justice, fairness and the rule of law – indeed, much of what the services exist to protect – risks being tarnished. Public confidence is being*

[225] *Ibid.*

[226] *Since 2004, the ISC has undertaken a number of investigations into these issues and has published two special reports on this subject ('The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq', Cm 6469, published in March 2005; and 'Rendition', Cm 7171, published in July 2007). In addition, on 17 March 2009, the Committee wrote to the then Prime Minister with its detailed findings regarding the case of Binyam Mohamed, a former Guantánamo Bay detainee ('Alleged complicity of the UK intelligence and security Agencies in torture or cruel, inhuman or degrading treatment'). In March 2010, the Committee reported to the Prime Minister on guidance on handling detainees ('Review of the Government's draft guidance on handling detainees'). Neither of these Reports has been published. The Committee has also provided updates on detainee-related issues, and the case of Binyam Mohamed in particular, in the Committee's 2008–2009 and 2009–2010 Annual Reports (Cm 7807 and Cm 7844 respectively).*

eroded, with people doubting the ability of our services to protect us and questioning the rules under which they operate. And terrorists and extremists are able to exploit those allegations for their own propaganda.[227]

209. In order to address the situation, the Prime Minister set out the following four measures:

i. settlement of the civil claims lodged by former Guantánamo Bay detainees against the Government in the High Court;

ii. a judge-led inquiry into the allegations of involvement or awareness of the UK intelligence Agencies in improper treatment of detainees held by third parties overseas;

iii. the publication of detailed guidance for intelligence and military personnel on how to deal with detainees held by other countries; and

iv. a Green Paper setting out the Government's proposals for how intelligence material should be treated in judicial proceedings.

(i) Settlement of civil claims from former Guantánamo Bay detainees

210. In April 2008, a number of former Guantánamo Bay detainees lodged civil claims for damages against the UK Government for alleged complicity in their detention, rendition and treatment by foreign powers (including US authorities). The Government intended to defend the claims and filed defences with the High Court.

211. Civil claims oblige all parties to disclose any documents held that are relevant to the claims. After reviewing the files, the Government had accumulated more than 500,000 documents which could potentially have to be disclosed. Each of these documents would first need to be reviewed by lawyers to determine their relevance and each would then need to be assessed in terms of national security sensitivities including, crucially, whether disclosure of the material might breach the 'control principle' (whereby intelligence from foreign liaison partners cannot be disclosed to third parties without the consent of the originator).

212. The scale of the task facing the Government was considerable. They estimated that the process would take years to complete and cost many tens of millions of pounds. More concerning was the fact that it was proving extremely difficult and time-consuming to attempt to protect sensitive intelligence material from court-ordered disclosure to the claimants and subsequently being placed in the public domain. (Whilst Public Interest Immunity, or PII, certificates can be used to protect sensitive material, it would have been an enormous exercise given the volume of material and it would have resulted in the exclusion of much of the key evidence and therefore the Government's ability to defend itself.)

[227] *HC Deb 6 July 2010 vol 513 c175.*

213. This lack of protection was particularly significant because some of the material in question was provided by foreign liaison partners. Disclosure of this information to the courts would have breached the 'control principle' and would have caused serious – and potentially irreparable – damage to intelligence-sharing relationships which are essential to the protection of UK national security.

214. The Government therefore decided that it would not be in the public interest to continue to seek to defend the claims and, on 6 July 2010, the Prime Minister announced that the Government would attempt to settle the claims out of court. On 4 November 2010, a settlement was agreed with 16 individuals. This included a binding agreement that all existing litigation would be halted, that no new claims would be launched and that the precise terms of the settlement would remain confidential.

215. Whilst the details of the settlement could not be made public, it was agreed that the Intelligence and Security Committee and the Chair of the Public Accounts Committee would see the details in order to provide the necessary Parliamentary accountability and scrutiny. On 5 November 2010, the National Security Adviser, Sir Peter Ricketts, wrote to the ISC to provide details of the settlement. He explained:

> *... the alternative to settlement of these cases was protracted and vastly expensive litigation in an uncertain legal environment in which the Government could not be certain that it would be able to defend the actions of the intelligence Agencies without compromising national security. The cases posed real concerns amongst key allies, particularly the US, about our ability to protect their secrets and stop them from ending up in the public domain. The Government has stated its commitment to drawing a line under the issues of the past raised by the Guantánamo claims and to enabling the intelligence Agencies to focus more fully on tackling the current national security threats we face. Successful settlement of these cases is an important step towards achieving those objectives.*[228]

216. On 16 November, the Justice Secretary announced the settlement in Parliament. He explained:

> *No admissions of culpability have been made in settling those cases and nor have any of the claimants withdrawn their allegations… Confidentiality was agreed by both parties, subject to the necessary parliamentary accountability and legal requirements… The alternative to any payments made was protracted and extremely expensive litigation… The cost was estimated at approximately £30 million to £50 million over three to five years of litigation.*[229]

217. The Committee notes that there is still one former UK resident detained in Guantánamo Bay. On 6 July 2010, the Prime Minister confirmed to Parliament that the Government would continue to make efforts to secure the release of Mr Shaker Aamer. The Foreign and Commonwealth Office wrote to the Committee in March 2011 to update us on the case. The Government has subsequently reaffirmed its commitment to securing Mr Aamer's return to the UK and has raised the matter with Secretary of State Clinton

---

[228] *Letter from the National Security Adviser, 5 November 2010.*

[229] *HC Deb 16 November 2010 vol 518 c752.*

and senior US officials on a number of occasions during the last year. The FCO has stated, however, that the decision is ultimately for the US to make and that this is complicated by restrictions on detainee transfers put in place by Congress in January 2011. At the time of writing, the Government continues to engage with US authorities seeking to secure Mr Aamer's return.

X. The Government's decision to settle claims by former Guantánamo Bay detainees was unpalatable to many. Nevertheless, in the circumstances it was the most sensible course of action. The resources required to defend these claims would have been substantially greater than the cost of the settlement, but more importantly the damage that would have been done to foreign liaison relationships would have left the UK vulnerable. We therefore conclude that it was overwhelmingly in the public interest that the cases were settled out of court. We note that the Government continues to engage with US authorities to secure the release of Shaker Aamer, the last remaining former UK resident in Guantánamo Bay.

(ii) Inquiry into the allegations of UK complicity in the improper treatment of detainees

218. Despite the settlement of these claims, there remained wider allegations and questions about UK complicity in the mistreatment and/or rendition of detainees. The ISC has produced two special reports on this issue, and a further two remain unpublished;[230] however, since the Committee in the last Parliament investigated these matters additional material has come into the public domain. The package of measures announced by the Prime Minister included a judge-led inquiry into the role of the UK Agencies. He told the House:

> *The longer these questions remain unanswered, the bigger the stain on our reputation as a country that believes in freedom and fairness and human rights. That's why I'm determined to get to the bottom of what happened. The intelligence services are also keen publicly to establish their principles and their integrity. So we will have a single, authoritative examination of all these issues…*
>
> *The inquiry will be able to look at all the information relevant to its work, including secret information; it will have access to all relevant Government papers, including those held by the intelligence services; and it will be able to take evidence in public – including from those who have brought accusations against the Government, and their representatives and interest groups…*
>
> *So I am confident the inquiry will reach an authoritative view on the actions of the state and our services, and make proper recommendations for the future.*[231]

[230] *See footnote 226 for details.*

[231] *HC Deb 6 July 2010 vol 513 c175.*

219. The inquiry panel comprises three Privy Counsellors: the former Court of Appeal judge, Sir Peter Gibson; the former Head of the Civil Service Commissioners, Dame Janet Paraskeva; and the former journalist and senior fellow at the Institute of Government, Peter Riddell.

220. The Prime Minister said that the inquiry would not begin until all related civil and criminal cases and investigations had concluded. While the civil cases were settled in November 2010, there were still two police investigations under way: one into the Security Service officer who interviewed Binyam Mohamed during his detention in Pakistan in May 2002, and one into the actions of an SIS officer.

221. In relation to the Security Service officer, known as 'Witness B', who interviewed Mr Mohamed after he had been deprived of sleep while in detention in Pakistan, the Director of Public Prosecutions announced on 17 November 2010 that "*there is insufficient evidence to prosecute Witness B for any criminal offence arising from the interview of Binyam Mohamed in Pakistan on 17 May 2002*". The Crown Prosecution Service announcement also indicated that there are some elements of the investigation that continue.

222. At the time of writing, there has been no announcement regarding progress on the separate investigation into the actions of the SIS officer.

(iii) Guidance on the handling of detainees

223. On 18 March 2009, as a result of the allegations, speculation and uncertainty surrounding the involvement of the intelligence and security Agencies and the Armed Forces in the treatment of detainees (including in the case of Mr Mohamed), the then Prime Minister announced to Parliament that:

> *We will publish our guidance to intelligence officers and service personnel about the standards that we apply during the detention and interviewing of detainees overseas once it has been consolidated and reviewed by the Intelligence and Security Committee. It is right that Parliament and the public should know what those involved in interviewing detainees can and cannot do. This will put beyond doubt the terms under which our Agencies and service personnel operate. Once published, copies will be placed in the libraries of the House.*[232]

224. Following this announcement, the Cabinet Office began the process of 'consolidating' the intelligence and security Agencies' and MoD's existing guidance. The ISC was provided with draft Consolidated Guidance in November 2009 and then undertook a detailed review, taking evidence from the Home Secretary, Foreign Secretary, Defence Secretary, Attorney General, Chief of SIS, Director General of the Security Service, Intelligence Services Commissioner, and the ISC Legal Advisor and Counsel. The ISC submitted its report *(Review of the Government's draft guidance on handling detainees*) to the then Prime Minister on 5 March 2010. Following a request by the then Foreign Secretary to clarify some of the issues dealt with in his previous evidence, the Committee submitted an addendum to the report on 12 April 2010.

---

[232] *HC Deb 18 March 2009 c55WS.*

225. The Committee's report includes detail on the legal and policy framework within which the Agencies and Armed Forces must operate, and analyses this against the operational imperative. It includes recommendations and conclusions on a number of matters, including Ministerial involvement and decision-making. A number of the Committee's recommendations were incorporated in the finalised guidance, which was published in July 2010. The Prime Minister did not publish the previous Committee's report since it related to the draft guidance rather than the final published version.

Y. The Committee welcomes the publication of the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*. It is essential that the Government's overarching policy in relation to detainees, upon which the lower-level practical guidance used by the Agencies is based, is set out clearly and unambiguously.

Z. Whilst the previous Committee's *Review of the Government's draft guidance on handling detainees* has not been published, we note that the recommendations and conclusions made by the Committee in the last Parliament were taken into account by the current Government in considering the guidance and have been – to some extent – reflected in the final version now published by the Prime Minister.

(iv) Green Paper on the protection of intelligence material in judicial proceedings

226. In its 2009–2010 Annual Report,[233] the ISC noted the ruling by the Court of Appeal in the case of Binyam Mohamed that resulted in a summary of classified US intelligence material being released into the public domain. The Court took this decision – in spite of submissions by the Government that it would damage national security – in part due to related information having been already placed in the public domain. However, the inability of the Government to prevent disclosure represented a breach of the 'control principle' which underpins the system of confidentiality upon which intelligence liaison relationships are founded. In its Report, the Committee said that it was:

> *… concerned that the publication of other countries' intelligence material, whether sensitive or otherwise, threatens to undermine the key 'control principle' of confidentiality which underpins relations with foreign intelligence services, and that this may seriously damage future intelligence co-operation.*[234]

227. The Prime Minister has acknowledged publicly the impact that the Court's decision has had on critical intelligence sharing relationships:

> *Today, there are serious problems. The services cannot disclose anything that is secret in order to defend themselves in court with confidence that that information will be protected. There are also doubts about our ability to protect the secrets of our allies and stop them ending up in the public domain. This has strained some of*

[233] *Cm 7844.*
[234] *Ibid.*

our oldest and most important security partnerships in the world – in particular, that with America. Honourable Members should not underestimate the vast two-way benefit this US–UK relationship has brought in disrupting terrorist plots and saving lives. So we need to deal with these problems… And next year, we will publish a Green Paper which will set out our proposals for how intelligence is treated in the full range of judicial proceedings, including addressing the concerns of our allies.[235]

228. The Committee has discussed the ramifications of the Court's decision with the Heads of the UK intelligence and security Agencies. The Chief of SIS told us:

There is no doubt that the Binyam Mohamed judgment of last February has affected the way in which ***.[236]

229. Similarly, the Director General of the Security Service told us:

***.[237]

230. In March 2011, the Committee visited the United States to discuss these concerns first-hand. We were struck by the force with which certain interlocutors within the US intelligence community voiced their worries about the actions of the UK courts, and we heard from a number of US agencies and departments that they viewed their material as ***.

231. ***. We have seen in the past how relatively insignificant pieces of background intelligence have, when connected together, provided important clues on individuals involved in extremism or terrorism. This is the fragmentary nature of intelligence: even the smallest piece of background intelligence can provide the critical piece of the jigsaw puzzle.

AA. We agree with the Government that the Court of Appeal's decision in the Binyam Mohamed case, which resulted in a breach of the 'control principle', has raised serious concerns which need to be resolved urgently. We therefore welcome the Prime Minister's announcement of a Green Paper setting out how intelligence material might be protected in judicial proceedings. The Committee will respond to those proposals in due course.

7/7 Inquests

232. On 26 November 2009, the Rt. Hon. Lady Justice Hallett (a senior Court of Appeal judge) was appointed Assistant Deputy Coroner with jurisdiction over the Inquests of those who lost their lives in the London terrorist attacks on 7 July 2005.

---

[235] *HC Deb 6 July 2010 vol 513 c175.*

[236] *Oral Evidence – SIS, 19 January 2011.*

[237] *Oral Evidence – Security Service, 9 February 2011.*

233. In May 2010, Lady Justice Hallett indicated the scope of the Inquests in a *Provisional Index of Factual Issues* which covered the following subjects:

- the deceased (backgrounds, personal evidence and movements on the day of the attacks);
- the explosions and the immediate aftermath;
- forensic issues regarding the bombs and the bodies of Mohammed Siddique Khan, Shehzad Tanweer, Hasib Hussain and Jermaine Lindsay (the four bombers);
- pathology issues;
- the backgrounds of Khan, Tanweer, Hussain and Lindsay; and
- preventability (including what was known about the four bombers prior to 7/7 and the alleged failings in the investigations conducted by the Security Service and the police).[238]

234. Given that the remit of the Inquests included the issue of 'preventability', the Coroner's team requested access to the classified versions of the ISC's reports on these matters.[239] In addition, the Coroner's team requested access to relevant extracts from transcripts of the Committee's evidence sessions with the Security Service, Metropolitan Police and West Yorkshire Police.[240]

Verdicts and Coroner's recommendations

235. On 6 May 2011, the Coroner delivered her verdicts and related findings. She ruled that all 52 victims had been unlawfully killed, and concluded that "*[no] failings on the part of any organisation or individual caused or contributed to any of the deaths*".[241] She therefore cleared the Security Service and the police of any shortcomings that could have prevented the attacks. Her conclusions were the same as those reached by the ISC in its 2009 report.[242]

236. The Coroner also acknowledged the pressure that the Security Service was under in the period prior to the 7/7 attacks – a point that the ISC had noted – and that resources had necessarily been deployed against higher-priority targets who were known to be involved in plans to attack the UK.

---

[238] *Letter from Coroner to Treasury Solicitors, 27 May 2010.*

[239] *'Report into the London Terrorist Attacks on 7 July 2005' (Cm 6785, published in May 2006) and 'Could 7/7 have been prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005' (Cm 7617, published in May 2009).*

[240] *Extracts from ISC transcripts of evidence were judged not to be relevant for disclosure in the Inquest proceedings themselves, although extracts from the Committee's reports were used.*

[241] *Coroner's concluding remarks, 6 May 2011, www.independent.gov.uk/7julyinquests*

[242] *Cm 7617.*

237. The Coroner made nine formal recommendations, of which two related to the Security Service:

- *I recommend that consideration be given to whether the procedures can be improved to ensure that 'human sources' who are asked to view photographs are shown copies of the photographs of the best possible quality, consistent with operational sensitivities.*
- *I recommend that procedures be examined by the Security Service to establish if there is room for further improvement in the recording of decisions relating to the assessment of targets.* [243]

BB. The Committee notes the Coroner's verdicts in the 7/7 Inquests, in particular that – as the ISC itself concluded in its 2009 Report – the Security Service and the police could not reasonably have prevented the attacks. The Committee supports the Coroner's recommendations that the Security Service should improve procedures for showing photographs to sources and that consideration be given to improving the recording of decision-making in relation to the assessment of targets. We have asked the Security Service to report to the Committee on plans to address these matters and will report the progress made in our next Annual Report.

Discrepancies in evidence

238. In addition to the Coroner's formal recommendations, she also noted that the ISC may have been "*inadvertently misled*" in relation to a small number of discrepancies between evidence prepared by the Security Service for the Inquests and evidence provided to the Committee. The Director General of the Security Service had already notified the Committee of these discrepancies, and offered the following explanation:

> *We cannot be sure that every individual point of detail included in the [Security Service's] Statement [to the Inquests] was passed to the Committee and it seems likely that in at least a few cases it was not. This is a result of the complexity and unsatisfactory state of our records during the period under review… I am certain that there was no deliberate intent to withhold information from the Committee, particularly in light of the unprecedented amount of operational detail that was shared.*
>
> *In constructing the Statement [to the Inquests] some instances have come to light where specific details included in the Committee's published report appear to be inaccurate. Some of these instances relate to marginal discrepancies over dates which may be down to human error. Others are more substantive and appear to be the result of either misunderstanding between the Service and the Committee (arising probably from the complexity and scale of information that was shared) or inaccurate, and incomplete, analysis of our records. For the Service's part, I regret these discrepancies and recognise the serious impact of such mistakes. Although human error is difficult to account for, I am confident that in terms of our information*

[243] *Coroner's Inquests, 'Report under Rule 43 of The Coroner's Rules 1984', 6 May 2011, www.independent.gov.uk/7julyinquests*

management and record keeping more generally we are in a stronger position today to avoid such issues arising in future investigations by the Committee.[244]

239. The discrepancies fall into two categories. The first relates to a number of minor inaccuracies arising from incorrect evidence being provided to the ISC, or insufficiently rigorous checks being undertaken when the Security Service was asked to check drafts for factual accuracy. As the Director General described in his letter, these particular discrepancies are likely to have arisen from oversights or human errors which, while disappointing, are to some extent understandable given the scale, scope and complexity of the Committee's investigation and some of the historical problems with Security Service records. Examples of this type of discrepancy include:

i. the fact that data relating to Mohammed Siddique Khan's mobile phone was obtained in March 2003, rather than in July 2003 as the Committee had been told; and

ii. the fact that Mohammed Siddique Khan, Shehzad Tanweer and an associate did not meet the terrorist facilitator, Mohammed Qayam Khan, at Toddington service station on 28 February 2004, as we were informed by the Security Service on various occasions that they had.

240. The second category of discrepancy is more serious, however. There are three instances where the Service did not provide the ISC with the relevant information at the time, or did not explain the information correctly.

i. Evidence given to the Committee at the outset of its investigation into the attacks said that "*the Service designates international terrorist targets for investigation as 'essential', 'desirable' or 'other'*". Subsequent evidence throughout both investigations continued to use these terms, and targets were routinely described as falling into one of these categories. The Committee specifically referred to the categories when asking whether particular information might have resulted in any of the bombers being placed under surveillance. However, in evidence to the Inquests the Security Service has explained that these categories were in fact used to explain their methodology to the Treasury and not by investigative officers. This is not the explanation provided to the ISC. We made this clear to the Security Service and asked for urgent clarification. The Director General conceded that "*on reflection, I accept that the lack of application of the categorisation system in a day-to-day context… was not made sufficiently clear in the Committee's final report*" and "*There was no attempt to mislead the Committee on this point but, on review of the relevant evidence, I believe that we should more clearly have emphasised to the Committee how the prioritisation system operated in practice.*"[245]

[244] *Letter from the Security Service, 27 January 2011.*

[245] *Letter from the Security Service, 6 April 2011.*

ii. Evidence given to the Inquests described how, in May 2005, a Security Service desk officer had speculated that some of the individuals from northern England, seen during Operation CREVICE, might be the targets of Operation DOWNTEMPO, who were thought to have attended training camps in Pakistan in 2003. Witness G said "*that was an intuition by the desk officer at the time…*".[246] Witness G accepted that, had this intuition been followed up, it would have made Mohammed Siddique Khan "*much more significant*".[247] However, he said that "*it would have been unusual to work further on that intuition because of the strong contra-indicators*".[248] The ISC was not provided with this information during its investigations into the 7 July bombings.

iii. During the course of the ISC's investigations into the 7 July bombings, all relevant exchanges between West Yorkshire Police and the Security Service were requested, and copies were provided to the Committee. The ISC noted that the Security Service had, on 16 February 2004, asked West Yorkshire Police whether they had any details of 'Hasina Patel', but that there was no response. The Committee questioned the Service about this and, when told that there was "*no record of a written response*", criticised the fact that the Security Service had not pursued the matter. However, evidence to the Inquests showed that there was a reply the following day, contrary to evidence given to the Committee.

241. The Coroner noted in her Rule 43 Report that these might be "*the result of the Service's poor record-keeping… at least one inaccuracy according to [Witness G, the Security Service's witness at the inquests] was because 'we didn't brief [the ISC] correctly'*".[249] She concluded:

> *It is essential that the ISC receives accurate information from the Security Service so that it can properly hold the Service to account, and report to the Prime Minister, Parliament and the public. It is, therefore, essential that great care is taken to check the draft reports for mistakes. Witness G accepted that the draft of the 2009 report was very important and had been sent to the Security Service to be checked for accuracy. He said it was checked to a very great depth, but 'not at a very high level'.*[250]

The Coroner expressed her expectation that "*consideration would be given to whether procedures can be improved to ensure the accuracy and completeness of information provided by the Security Service to the ISC*".[251]

---

[246] *Witness G's evidence to the 7 July Inquests, 23 February 2011, www.independent.gov.uk/7julyinquests*

[247] *Ibid.*

[248] *Ibid. These included the fact that detainees involved in these training camps had failed to identify the men from photographs taken during Operation CREVICE and therefore there was no intelligence to suggest that the men might be the targets of Operation DOWNTEMPO.*

[249] *Coroner's Inquests, 'Report under Rule 43 of The Coroner's Rules 1984', 6 May 2011, www.independent.gov.uk/7julyinquests*

[250] *Ibid.*

[251] *Ibid.*

242. The ISC has both publicly and in private highlighted the serious problems with the Agencies' record keeping and the accuracy of information provided to us. In its 2008–2009 Annual Report, the ISC said:

> *One of the issues arising from the Mr Mohamed case is the fact that relevant documentation was overlooked. The Security Service failed to discover all the relevant information when searching its records for this Committee's Rendition inquiry (in 2007). Further relevant documents were discovered during searches of its records for Mr Mohamed's case in the High Court (in 2008). During 2009, a further 20 documents relevant to Mr Mohamed's case were discovered, two of which were identified as a result of this Committee's questioning of the Agencies (which, in turn, prompted a further review which led to the disclosure of an additional seven documents).*
>
> *… the Director General of the Security Service has told us:*
>
> > *The information in question should have been found when we… carried out wide-ranging searches of records at the time of the Committee's inquiry into rendition… I cannot fully explain why it was not discovered in… our… records… Service systems in place at the time should have located this information.*
>
> *… There is no convincing explanation as to why this information was not made available… While we do not believe that this was a deliberate attempt to deceive us, it highlights fundamental problems with the record-keeping systems and processes of both Agencies.*
>
> *… While we understand that the balance of the Agencies' effort must be focused on operational work, at the same time good record keeping is crucial. The Agencies' operational work is about knowledge and information, and the ability to retrieve such information is central to the work with which they are charged. We welcome the assurances we have received from the Security Service and Secret Intelligence Service that they are taking action to rectify the problems with their records, although we note that it will take several years before new systems are fully established. This has serious ramifications – both in terms of the Agencies' own work and for the reliability of the evidence they submit to this Committee.*[252]

243. In March 2009, when the ISC wrote to the then Prime Minister regarding allegations of UK complicity in the mistreatment of Mr Binyam Mohamed, we again highlighted the problems we had encountered with the proper provision of information. The Committee said:

> *We have been told, repeatedly, that steps are being taken to improve the Agencies' record-keeping. However, in the meantime we are being told that information provided to the Committee may not be complete. This is demonstrated by a recent letter from SIS to the Committee, regarding allegations that UK Agencies had been*

[252] *Cm 7807.*

involved in the rendition, from Somalia to Ethiopia, of a number of individuals. The information provided by SIS was accompanied by a caveat:

> *However, as demonstrated in the recent Mr Mohamed case, it cannot be ruled out that searches carried out using different search parameters, for example, in connection with any future court proceedings in the UK, might unearth additional information.*

This Committee believes that the use of such a caveat is completely unacceptable. It undermines the ability of the Committee to do the job it was established by statute to perform.

The Agencies must conduct thorough research in support of any information provided to the Committee. When information emerges after the Committee has reported on a matter, it damages trust in this Committee, undermines our credibility and harms democratic accountability. It gives fuel to those who argue that the ISC does not have sufficient authority to conduct its inquiries and supports their calls for full public or judicial inquiries. Indeed a letter from Andrew Tyrie MP to the Committee of August last year said in relation to this case:

> *... if it were to transpire that you are unable to rely on information provided to you by the Agencies then the value of the Committee would be called into question.*

If all branches of Government cannot keep this Committee properly informed, oversight of the Agencies will inevitably be played out through the courts, as we have seen in this case.[253]

244. The Agencies have acknowledged problems in this area and have taken steps to improve their record keeping and information management.[254] However, this is forward-looking and therefore we assess that there may be continuing problems in relation to searching historical records.

CC. We have identified eight examples where there were very minor inaccuracies or inconsistencies in evidence given to the ISC, compared with evidence subsequently provided to the Coroner. We have also identified three discrepancies which are more significant. These are extremely frustrating for the Committee, and for those who rely on our reports. We have satisfied ourselves, however, that they do not alter the conclusions and recommendations that were made in the Committee's *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*.

DD. The Coroner in the 7/7 Inquests acknowledged that the ISC's second report on the 7 July 2005 terrorist attacks was "*detailed and thorough*". However, she also noted the discrepancies between evidence to the ISC and that given to the Inquests, and criticised the Security Service for their poor record keeping. We share her concerns, having previously made the same point ourselves to the Agencies and to

---

[253] *Letter to the Prime Minister, 17 March 2009.*

[254] *Further details on the Agencies' investment programmes can be found at paragraphs 79 to 81 (Security Service) and 106 to 108 (SIS).*

the two previous Prime Ministers. It is essential that the intelligence community make greater efforts to ensure that information provided to this Committee is full and accurate, that searches in response to Committee requests receive the same attention as requests from the courts, and that draft reports are reviewed properly, to ensure that such problems do not arise again.

BBC Monitoring

Background

245. BBC Monitoring (BBCM) was established in 1939 and provides global reporting and analysis of open source media to customers including the FCO, the MoD, the intelligence and security Agencies, the Cabinet Office and BBC World Service. It monitors around 15,000 media sources across 150 countries in 100 languages and delivers approximately 1,000 products per day. BBCM has a close partnership with the US Open Source Center (OSC), which is hosted by the Director of National Intelligence. Given the far greater size and capability of the OSC, this provides a large source of unfunded benefit to the UK through the free reciprocal interchange of product.

246. The ISC has previously taken an interest in BBC Monitoring given the use that the intelligence community make of its open source product. In 2003 – when BBCM's funding came under threat – the Committee reported that "*BBC Monitoring provides a valuable service both to government departments and to the Agencies*" and recommended that BBCM's "*overall level of funding should reflect the value of BBC Monitoring to Government, the Agencies, and US relationships as a whole*".[255]

247. As a result of these concerns, the Cabinet Office commissioned a strategic review of BBCM. The review – conducted by Sir Quentin Thomas – reported in 2005, concluding that BBCM's open source material was valuable to the UK Government and the intelligence Agencies, and emphasised the importance of its relationship with the US Open Source Center. The Review concluded that:

> *If this monitoring service were brought to an end the product would not be available from alternative sources. Moreover it would prove a false economy because steps taken by present stakeholders to remedy its loss, or to manage without it, are likely to be more costly.* [256]

248. The Review advocated stable and adequate funding for BBCM of £24.6m per year until 2011 and recommended that HMG's contribution to BBCM's funding should be ring-fenced and administered centrally by the Cabinet Office, which should act as BBCM's sponsoring department. The Government broadly accepted these recommendations and a new governance regime was put in place, with a Stakeholder Board[257] established to determine strategic direction and priorities and a Memorandum of Understanding (MoU) signed by BBCM's stakeholders.

---

[255] *Cm 6240.*

[256] *Sir Quentin Thomas, 'Review of BBC Monitoring', 2005.*

[257] *BBC Monitoring's Stakeholder Board includes representatives from BBCM, BBC World Service, the Cabinet Office, Foreign Office, MoD and the intelligence Agencies.*

Cabinet Office cuts

249. In April 2010, BBCM and its stakeholders were informed that the Cabinet Office Executive Board had removed £1.4m per annum (8% in real terms) from the BBCM budget for 2010/11. BBCM has told us that the decision was taken without prior consultation with BBCM, its customers or stakeholders.[258] The Cabinet Secretary later admitted that BBCM's funding had ceased to be ring-fenced from the Cabinet Office budget, and that there was no Ministerial sponsorship of BBCM.[259] This was in direct contravention of the MoU governing BBCM's relationship with its stakeholders. The Cabinet Secretary later said that "*how this came about, given the structures set out in the earlier Memorandum of Understanding, is not clear*".[260] However no steps were taken to rectify the situation and in October 2010, the Deputy National Security Adviser admitted that "*it sounds rather a sorry story*".[261]

2010 Spending Review

250. BBCM was subsequently informed (later in April 2010) by the Cabinet Office that its newly reduced budget of £23.2m per annum would now serve as its baseline for the Spending Review, raising the prospect of further cuts. BBCM warned that further cuts could threaten its very existence and that it could "*cease to be a going concern before the end of the SR period, running out of cash and folding under the pressure on its budget*".[262]

251. BBCM's stakeholders submitted a Spending Review bid to the Cabinet Office setting out BBCM's value to the UK, both directly as the UK's only taskable open source asset, and as a result of its partnership with the OSC which brings wider benefits to the UK in its intelligence and security relationship with the US. The Director of the OSC wrote in support of the bid, saying:

> *I would like to emphasize the immense contribution BBCM makes to the US intelligence and policy communities, as well as to the overall US–UK special relationship… In short, OSC cannot fulfil its mission without the unique material and expertise BBCM provides – prime examples among many being the Russia–Georgia conflict and the Iran post-election crisis.*[263]

252. When the outcome of the 2010 Spending Review was announced, the Government said that it had "*agreed with the BBC that the TV licence fee will fund BBC World Service, BBC Monitoring, and S4C*".[264] Dr Chris Westcott, the Director of BBC Monitoring, welcomed the stability offered by the move to funding by the BBC licence fee from 2013, although details of the interim funding arrangements had not, at that time, been agreed.

253. When the Committee questioned the National Security Adviser about the future for BBC Monitoring he said that:

---

[258] *Letter from Dr Chris Westcott, Director of BBC Monitoring, 8 July 2010.*

[259] *Ibid.*

[260] *Quoted in a letter from Dr Chris Westcott, 24 September 2010.*

[261] *Evidence from the National Security Adviser and Deputy National Security Adviser, 21 October 2010.*

[262] *Letter from Dr Chris Westcott, 24 September 2010.*

[263] *Quoted in a letter from Dr Chris Westcott, 24 September 2010.*

[264] *Cm 7942.*

I don't think that it's ever been a very happy position for the budget of the BBC Monitoring to be part of the Cabinet Office budget. I think what the difficulties of the last few years … have shown is that it wasn't a natural place to lodge the funding for the BBC Monitoring, frankly. I think it is in the better long-term interests of [BBCM] to be part of the BBC family, with the right appropriate governance arrangements... because at the end of the day they are all part of the BBC family. So I think we should be able to make this work in a way that the staff will feel is better... we will take our transitional responsibilities very seriously. [265]

254. The Deputy National Security Adviser added that:

... the Cabinet Office's duty over the next couple of years, while we retain ownership of it, is to sort out a sensible transitional mechanism that keeps the service at roughly the levels it is now, before it transfers over to the financial responsibility of the BBC... So there are two more years in which [the Cabinet Office has] a custodian duty towards BBC Monitoring… Our very strong intention is to use the period between now and 2013 to make sure that we have binding commitments from the BBC… You can never say absolutely never when you are transferring something out of your direct control, but we would hope to bind them in writing to a given service level… I intend to achieve that.[266]

255. In January 2011, BBCM announced that the Cabinet Office was making further cuts to the BBCM grant prior to the transfer to licence fee funding. Dr Westcott wrote to inform the Committee that:

BBC Monitoring is today announcing spending cuts and proposed post closures in response to the decision by the Cabinet Office, following last October's… Spending Review, to cut £3m per annum (18%) over two years from BBC Monitoring's grant of £23.2m per annum. This follows a cut of £1.4m by the Cabinet Office in April 2010. In announcing the cuts to staff today, I will be saying that regrettably service cuts and post closures are inevitable given the scale of the cut in funding from the Cabinet Office… BBC Monitoring proposes to cut £3m per annum from its costs by closing 72 posts – about 16%.[267]

EE. BBC Monitoring provides an irreplaceable service to the intelligence community, and offers considerable value for money due to the free flow of information with its far larger US counterpart. It is therefore of considerable concern to the Committee that its funding was arbitrarily cut without consultation in April 2010, in direct contravention of the governing Memorandum of Understanding, and that it now faces further cuts over the next two years. The Foreign Affairs Committee has already recommended revisiting the decision about the BBC World Service's funding,[268] and we note the Government's decision to give an extra £2.2m to maintain Arabic services. There is also a powerful case for reviewing the decisions that were made about BBC Monitoring's funding in the 2010 Spending Review. The

[265] *Oral Evidence – National Security Adviser and Deputy National Security Adviser, 21 October 2010.*

[266] *Ibid.*

[267] *Letter from Dr Chris Westcott, 17 January 2011.*

[268] *HC 849, 13 April 2011.*

National Security Adviser must ensure that BBC Monitoring is able to maintain the level of service required by departments and Agencies. We strongly recommend that Ministers reconsider the cuts to BBC Monitoring in the period leading up to the transfer to licence fee funding.

Collaborative working

256. The ISC has for a number of years recommended that the Agencies explore ways of working together more closely – not just on operations, where the benefits are clear, but also on administrative or corporate services where there is scope for more effective working and for cost savings. The 2010 Spending Review – which imposed real-terms cuts on the Agencies of 11.3% over the Spending Review period – acknowledged that "*Greater collaboration between the three Agencies will make them more effective in their work, but also secure financial savings*".[269] The Heads of the Agencies have all recognised that collaborative working is going to be key to achieving the savings required.

Operations

257. The Agencies have already made progress with regard to operational joint working. The Security Service has told the Committee that since April 2009 "*there have been significant developments on collaborative working across the SIA*" and that this has been built on "*the close operational relationships that have been a feature of our work over many years*".[270] The Chief of SIS told the Committee that:

> *The greatest benefit of collaborative working is improving the productivity of the Agencies' [operational] work. When we bring SIS and GCHQ teams together, they see very clearly how they can help one another, how they can produce a more joined-up approach, they can cover targets more efficiently, and SIS can facilitate GCHQ operations and GCHQ can facilitate SIS operations.*[271]

258. Examples of collaborative operational work include the establishment of a tri-Agency team to pursue terrorist threats upstream, and work being undertaken by GCHQ and the Security Service to develop a joint approach on internet-related work.

Corporate services

259. During 2009/10 a Director of Collaborative Working was appointed by the three Agencies. This post, supported by a small tri-Agency team, set out to identify and exploit opportunities for collaborative working. A number of areas have been identified:

- a joint approach to planning investment in capabilities;
- a joint SIA UK estates strategy;

---

[269] *Cm 7942.*

[270] *Letter from the Security Service, 16 September 2010.*

[271] *Oral Evidence – SIS, 19 January 2011.*

- increased sharing in the delivery and running of IT; and
- a move to significant sharing of corporate services.

260. The Director General of the Security Service gave a practical example of how savings were now being made as a result of a joint approach by the three Agencies:

> *We applied what is known in the trade, I understand, as a haircut… We went with SIS and GCHQ to all of our IT contractors and said… 'You are all going to work off the bottom rate that any of the Agencies has got, and we are going to take 10 per cent off that. There's nowhere to go because all the Agencies are doing it, and therefore you can't run to the other Agency and say, 'we would like to work a bit more for you''.*[272]

261. The Committee questioned the Agencies on the scope for further joint working, particularly in relation to language training and vetting.[273] With regard to language training and foreign language provision, the Agencies appear to be making good progress, with joint attendance on language courses, a joint tendering process and the establishment of a joint language centre hosted by the Security Service, which has boosted intelligence-producing capacity. The Director of GCHQ told us that:

> *We have developed a joint tendering process to ensure that Agencies achieve competitive rates from the external language training providers. The Security Service and SIS requirements are included in our contract… Each Agency routinely offers places on its language training and enhancement courses to its counterparts.*[274]

262. While such examples represent a good start, the Chief of SIS warned the Committee that there are limits to the savings that can be achieved:

> *All three Agencies have had their SR10 settlements based on cutting the administration costs of the Agencies by 33.3 per cent, by one-third. We can do that internally or we can do it through collaboration, but we can't do it twice. We can't save 33.3 per cent internally and then save another chunk by collaborating with one another. That is a bridge too far.* [275]

FF. The Committee welcomes the greater emphasis now being put on collaborative working, both in terms of operational work and corporate services: the Agencies must explore all opportunities to make savings if they are to safeguard their core capability. They have made a good start and we encourage them to maintain this momentum.

---

[272] *Oral Evidence – Security Service, 9 February 2011.*

[273] *Vetting is covered further in paragraphs 266 to 269.*

[274] *Oral Evidence – GCHQ, 3 February 2011.*

[275] *Oral Evidence – SIS, 19 January 2011.*

Business continuity

263. Last year the Committee reported that the Security Service and SIS were planning to establish a Joint Data Centre to provide secure storage outside London for their data.[276] We have been updated on the project this year as plans have progressed.

264. Once this facility is completed it will allow access to current and archive data should the Agencies' primary premises be rendered unusable. For SIS in particular, this will overcome the shortcomings that the ISC has previously identified in their back-up arrangements. The Chief of SIS told us that:

> *When it's fully up and running… if, for example, Vauxhall Cross is unusable, at the moment, under our present arrangements, there will be a… gap in the data available to us. Once this is up and running and, say, we have to move to [our back-up site] for whatever reason… we will have immediate access to all the material in the Joint Data Centre, without gap.*[277]

265. The ISC in the last Parliament noted that GCHQ was not – at least in the short term – taking part in this project despite the fact that it is vulnerable because so much of its key operational equipment is located in the Cheltenham area.[278] GCHQ has said that this was because the site did not have sufficient capacity to meet its requirements. This year, we have questioned GCHQ as to how it proposes to address this vulnerability. We were told that GCHQ is examining alternative options for additional data centre space, but could not give any firm timescale for when this might take place. GCHQ also told us that:

> *GCHQ and the Security Service are putting a programme of work in place to do a substantial amount of collaboration on the provision of IT Services and a core infrastructure between those two Agencies with a view that SIS will join that in due course, towards the end of the spending review period. Part of that work will be to develop a data centre strategy, including a resilience strategy for the three Agencies. So at present we do not believe that the current design [of the joint data centre] would improve our resilience in the way it is currently being implemented, but we are working with them in terms of developing this collaborative security resilience strategy for our data centres in due course.*[279]

GG. Although GCHQ has taken steps to reduce its vulnerability to disruptive events – for example through the planned closure of the less-resilient Oakley site – the Committee is very concerned that the lack of a back-up data centre leaves GCHQ exposed should its primary site be out of action. GCHQ should therefore bring forward specific proposals to address this risk at the earliest opportunity.

---

[276] *Cm 7844.*

[277] *Oral Evidence – SIS, 19 January 2011.*

[278] *Cm 7807.*

[279] *Oral Evidence – GCHQ, 3 February 2011.*

Vetting

266. All staff working for the Agencies are subject to a regime of Developed Vetting, a process of background checks that takes several months to complete and costs several thousand pounds. In February 2010, the ISC in the last Parliament tasked its Investigator with conducting an inquiry into national security vetting in the intelligence and security Agencies in order to explore whether there are opportunities for closer co-operation between the Agencies which could make the process of vetting more streamlined and efficient whilst reducing costs.

267. The Investigator's report concluded:

> *No vetting system is foolproof but robust and comprehensive processes can certainly lower the chance of employing a security risk in a particular organisation or post. The intelligence Agencies pride themselves on having in place such robust and comprehensive vetting processes. There is no reason to doubt that this is so… national security vetting in the Agencies is focused and rigorous.*[280]

268. At the same time, however, the Investigator noted that there were some areas where changes could be made to align the three Agencies' work in this area more closely "*to help justify or eliminate differing processes or standards and to allow choices to be made about more efficient systems*".[281] The Investigator made 11 recommendations that would achieve this, building on the close co-operation that was already apparent between the Agencies. One of these was that the Agencies "*should adopt aligned vetting processes*".[282]

269. We have questioned the Agencies on the potential of a single vetting system. SIS noted:

> *There isn't as yet, as I understand it, a plan to have a completely merged single team, but there is a level of collaboration, consistency of standards, accepting of each others' vetting clearances.*[283]

The Director of GCHQ told us that:

> *I think our assessment has been that GCHQ vetting is… not costing more than it would under a single Agency solution; and whilst single vetting is viable in the early stages, the departments will wish to retain responsibility for making [their] decisions on who to bring [in] and for managing aftercare.*[284]

However, the Director General of the Security Service said:

> *From my point of view, I would be quite happy to have a single vetting unit.*[285]

---

[280] *ISC Investigator Report – National Security Vetting in the Intelligence Agencies, June 2010.*

[281] *Ibid.*

[282] *Ibid.*

[283] *Oral Evidence – SIS, 19 January 2011.*

[284] *Oral Evidence – GCHQ, 3 February 2011.*

[285] *Oral Evidence – Security Service, 9 February 2011.*

HH. The Committee accepts that there is a strong case for the Agencies to conduct vetting separately from other parts of government. However, there remains no convincing argument as to why each of the Agencies should maintain separate systems. A single organisation conducting vetting on behalf of all three, with the process tailored to each Agency's specific requirement, would offer considerable benefit. We recommend that the Agencies investigate this as both desirable in its own right and as a potential contribution to their savings targets during the 2010 Spending Review period, and await their response.

SECTION 7: OVERSIGHT

Reform of the ISC

270. In the 16 years since the Intelligence and Security Committee was established there have been a number of changes within the intelligence community, and the work of the Committee has evolved to take account of these. However, public expectation in terms of transparency and openness has increased significantly during this time, and the Committee must ensure that it has the powers and remit that are necessary to provide reassurance to the public and to Parliament.

271. The ISC in the last Parliament stated in its 2009–2010 Annual Report that it was "*confident in its ability to hold the Agencies, and other bodies with an intelligence role, to account and to do so independently of Government*". However it noted that "*Nevertheless, over the last six months, questions have been raised about the independence of the Committee*". This led the Committee to revisit those principles, policies and procedures which govern the work, status, remit and responsibility of the Committee and under which the Committee operates. It believed that corporate knowledge of the Committee's procedures within government had been lost over time and that this had led "*in some cases to misunderstandings as to the statutory independence of the Committee and its work and the nature of the relationship between the Committee and the Prime Minister*". In reviewing its procedures, the Committee was clear that it was no longer appropriate for it to be hosted by the Cabinet Office if there was to be confidence in the independence of the Committee. The Committee said that "*As a matter of principle, no matter what the circumstances, it clearly is not right to be hosted by an organisation that you have some role in overseeing and there is a danger that boundaries might not be respected*". It concluded that the *status quo* was unsustainable.

272. This Committee agrees with its predecessor that it is essential that it is able to provide credible reassurance both to the public and to Parliament that, consistent with necessary secrecy and security, the Agencies operate in the public interest. We have therefore made it a priority this year to conduct a root-and-branch review of the Committee's role, structure, remit and powers. We took the 1994 legislation that established the ISC as our starting point, and examined whether it reflected how the Committee's work has evolved over the past 16 years and whether it provided the greater openness and transparency that is now necessary.

273. We concluded that the current arrangements are significantly out of date. The Committee's remit and powers have evolved beyond the *de minimis* position set out in the 1994 Act: the Committee today takes evidence from other parts of the intelligence community rather than just the three Agencies, and has retrospectively reviewed specific operations as well as the administration, policy, and expenditure that the Act makes provision for. The legislation also contains safeguards that – whilst they were thought necessary in 1994 – are now outdated, including the limited power of the ISC to request, rather than require, information from the Agencies. The 1994 Act therefore requires updating.

274. The Government's Green Paper on the protection of intelligence material in the courts provides an excellent opportunity for legislative change. Indeed if the Government is to recommend changes in the powers of the courts, then it is essential that oversight of the Agencies is strengthened. We have produced radical proposals for change, designed to increase accountability, transparency and capacity for oversight of the intelligence community. Our detailed proposals – which we believe should form the basis for the relevant parts of the Green Paper – were put to the National Security Adviser on 31 March 2011.

II. The Intelligence and Security Committee was established under the Intelligence Services Act 1994, and has now been in existence for over 16 years. We therefore considered that it was right to review whether the structure, remit and powers of the Committee were still sufficient in the context of the current intelligence machinery. It is clear that the current provisions are outdated and that the *status quo* is unsustainable. We have therefore submitted radical proposals for change that will ensure strengthened, more credible oversight of the UK intelligence and security Agencies and provide greater assurance to the public and to Parliament. We recommend that these form the basis for the proposals for reform of the ISC in the forthcoming Green Paper on the handling of intelligence material in judicial proceedings.

JJ. Our proposals to the National Security Council are based on the following key principles:

- **the Intelligence and Security Committee should become a Committee of Parliament, with the necessary safeguards, reporting both to Parliament and the Prime Minister;**
- **the remit of the Committee must reflect the fact that the ISC has for some years taken evidence from, and made recommendations regarding, the wider intelligence community, and not just SIS, GCHQ and the Security Service;**
- **the Committee's remit must reflect the fact that the Committee is not limited to examining policy, administration and finances, but encompasses all the work of the Agencies;**
- **the Committee must have the power to require information to be provided. Any power to withhold information should be held at Secretary of State level, and not by the Heads of the Agencies; and**
- **the Committee should have greater investigative and research resources at its disposal.**

The Investigatory Powers Tribunal and the Commissioners

275. The Committee met the Investigatory Powers Tribunal, the Interception of Communications Commissioner and the Intelligence Services Commissioner on 24 March 2011. The Committee meets the Commissioners on an annual basis for an informal discussion about their respective roles. This is the first occasion on which we have met the President of the Investigatory Powers Tribunal.

276. The main function of the Interception of Communications Commissioner, appointed under section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA), is to review:

- the exercise and performance of the Secretary of State's powers conferred on him or her in authorising interception warrants;
- the exercising of powers and duties in relation to the acquisition and disclosure by public authorities of communications data; and
- the exercising of the Secretary of State's powers and duties in relation to the investigation of electronic data protected by encryption.

277. The main functions of the Intelligence Services Commissioner, appointed under section 59 of RIPA, are to keep under review:

- the exercise by the Secretary of State of his or her powers to issue, renew, and cancel warrants for entry on, or interference with, property or with wireless telegraphy;
- the exercise by the Secretary of State of his or her powers to authorise acts done outside the UK, which may be unlawful without such an authorisation;
- the exercise and performance of the Secretary of State's powers and duties in granting authorisations for intrusive surveillance, and the investigation of electronic data protected by encryption; and
- the exercise and performance by members of the intelligence Agencies of their powers and duties under Parts II and III of RIPA, in particular with regard to the grant of authorisations for directed surveillance and for the conduct and use of covert human intelligence sources and the investigation of electronic data protected by encryption.

278. Both Commissioners visit the Agencies at least twice a year to conduct inspection visits, where they review the use of warrants and authorisations in the context of associated operational activities. They examine all relevant documents, and discuss the cases with the officers concerned to ensure compliance with the relevant safeguards and the Codes of Practice. Both Commissioners stated that they were content that the responsibility is taken very seriously by officials and that sufficient attention to submissions is given by Ministers. They also said that the Agencies are keen to comply and that they will sometimes even seek advice from the Commissioners in advance of an application.

279. Like the ISC, the Prime Minister has on occasion asked the Commissioners to take on duties in addition to their statutory remit. As Intelligence Services Commissioner, Sir Peter Gibson was asked to report on the Agencies' compliance with the Consolidated Guidance on Handling Detainees. His findings will be published in the next Intelligence Services Commissioner's Annual Report.[286]

280. The Commissioners report annually to the Prime Minister. However, unlike the ISC, their reports are not redacted, but classified information is contained in a separate annex to the report which is not published. Since 2002, the Committee has sought access to these classified annexes from the Government without success. Both Commissioners have informed the Cabinet Office that they have no objection to the Committee having access to the annexes and the National Security Adviser has now agreed to review the matter.

281. The Investigatory Powers Tribunal was established to investigate complaints about the conduct of the intelligence and security Agencies (and other public bodies) relating to the exercise of powers under RIPA. All organisations holding such powers have a legal obligation to provide the Tribunal with assistance to conduct its investigations. The Tribunal consists of ten members, headed by a President (Lord Justice Mummery) and a Vice-President.

282. This was the first time that the Committee had an opportunity to hear about the work of the Investigatory Powers Tribunal and it was very useful to understand how the Agencies engage with the Tribunal and compare that with our own – and the Commissioners' – experience.

[286] *Sir Peter Gibson stood down from this position on December 2010, and was succeeded by Sir Mark Waller.*

SECTION 8: RECOMMENDATIONS AND CONCLUSIONS

A. Given the scale of the spending cuts across government, we recognise that the intelligence and security Agencies received a fair settlement in the Spending Review. Nevertheless, we are concerned that an 11.3% reduction in budgets will inevitably have an impact on the ability of all three Agencies to maintain current levels of coverage of all aspects of the threat, and that this may worsen if inflation remains at its current levels. This will require tough decisions in the coming years.

B. Given the importance of national security work, it is essential that the Spending Review settlement can be adjusted if there is a significant change in the threat. The Committee will keep this under review.

C. GCHQ's Corporate Technical Investment Portfolio (CTIP), of which SIGMOD is part, accounts for a significant proportion of the SIA expenditure. It is a complex set of programmes that encompasses most of GCHQ's work. The Committee has therefore tasked its Investigator to scrutinise CTIP's structure and overarching governance and report to us his findings. This investigation is now under way. We have also asked the National Audit Office to examine specific projects under the SIGMOD banner in due course, to assess the value for money they offer.

D. The Committee is disappointed that government departments and agencies do not view investment in Information Assurance as important, and that this has led to GCHQ having to subsidise CESG by several million pounds per year. We are concerned that there appears to have been little progress in achieving a resolution since last year. The Deputy National Security Adviser must prioritise the development of an effective funding model, which should be implemented within the next six months.

E. We are concerned about GCHQ's inability to retain a suitable cadre of internet specialists to respond to the threat. We therefore urge GCHQ to investigate what might be done within existing pay constraints to improve the situation. We also recommend that the Cabinet Office – as lead department for cyber security – considers whether a system of bonuses for specialist skills, such as exists in the United States, should be introduced.

F. The Committee welcomes the savings that will accrue from the disposal of GCHQ's London office and Oakley site. However, we remain concerned that GCHQ's accommodation strategy has been haphazard in the past and, with the current rationalisation taking place, lacks any flexibility for the future. The GCHQ Board must plan better for the future and develop a sensible long-term strategy for its accommodation requirements.

G. The Committee is concerned that, over a prolonged period, GCHQ has been unable to account for equipment worth up to £1m. Assets must be monitored effectively and controls must be in place to ensure that public money is not wasted. Whilst the majority of the items that could not be traced attracted no security risk, GCHQ has admitted to us that it cannot guarantee that this is the case for 5% (or 450) of these items. Although the Committee has no reason to believe national security has been compromised, the

Agencies must do all they can to avoid the loss of potentially sensitive equipment. The public interest requires that GCHQ learns from the repeated mistakes of the past. The Committee expects GCHQ to ensure that the situation does not arise again.

H. The Committee welcomes the improvement by the Security Service in managing 'end-year surges'. However, we urge the Service to implement the recommendation of the National Audit Office to improve their forecasting processes in order to manage expenditure evenly throughout the financial year.

I. The Security Service has told the Committee that it has been able to respond effectively to the recent increased threat in Northern Ireland. Nevertheless, given the increase in the number of attacks, it is clear that further sustained effort will be required. In the context of declining resources, this will affect the Service's capability in other areas, which is a matter for concern.

J. The Service is already focused on planning around the 2012 Olympic Games. The Director General has told us that he considers the Service to be well placed to manage the risks that the Olympics will bring. The Committee is nevertheless concerned that this will inevitably divert resources from the Service's other work during this period, and thus expose the UK to greater risk. The National Security Council must take such steps as are necessary to minimise the risk to the UK.

K. The Committee recognises that the Security Service needs IT specialists in order to deliver its major technology projects. However, spending on consultants and contractors continues to increase at a significant rate. The Service should consider whether collaborative working – with GCHQ in particular – could provide some savings in this area. The Committee will examine the Agencies' use of consultants and contractors in greater detail over the coming year.

L. This is the fourth consecutive year that SIS has failed to manage its expenditure effectively throughout the year and has seen an 'end-year surge'. The Intelligence and Security Committee has consistently been critical of this, agreeing with the National Audit Office's view that it increases the risk of inefficiency and lack of value for money. The Committee expects SIS, in the current financial climate, to ensure that it manages its budget sensibly in future and will monitor whether this is happening during the current financial year.

M. The Committee welcomes the establishment of the National Security Council. It is important that there is a forum that meets regularly to enable Ministers to take decisions on national security matters and that provides an opportunity for more regular contact between Ministers and the Heads of the Agencies. The NSC must retain its current status and priority.

N. The Committee welcomes the fact that – through the National Security Strategy – the requirements process which determines the intelligence and security Agencies' allocation of effort is now given greater priority. It will be important, however, to ensure that threats lower down the hierarchy are still given appropriate attention.

O. The Committee welcomes the creation of the National Security Adviser post, and the review of the central security and intelligence structures. As part of this review, the different sets of targets, requirements, priorities and objectives that the Agencies are subject to must be reviewed and simplified: there must be one clear tasking process. In particular, it is important that the work of the Joint Intelligence Committee, and the Requirements and Priorities process, is aligned with the strategic direction being set by the National Security Council.

P. The Committee remains concerned about the overlap in remit and potential for duplication of work between the Office for Security and Counter-Terrorism and the National Security Secretariat in the Cabinet Office. Since central structures are currently being examined, we recommend that thought is given to OSCT's future role in the light of that review.

Q. The Committee accepts that it is not easily achieved, but it is nevertheless essential that there is some mechanism by which the success of work on the PREVENT strand of CONTEST – and the benefits of RICU in particular – can be evaluated.

R. The Committee notes the assurance provided by the Director General of the Security Service that, with additional funding and the measures included in the Terrorism Prevention and Investigation Measures Bill, there should be no substantial increase in overall risk. However, any increase at all in the overall threat to national security would be a matter of serious concern. The Committee will take further evidence on the impact of the new regime in due course.

S. Counter-Terrorism work must be effectively co-ordinated and there must be a clear strategy. Work falling under CONTEST has been subject to a number of separate reviews over the last year. The Government must ensure that these do not operate in isolation from each other and that the end result is properly co-ordinated.

T. It is disappointing that the Strategic Tasking Directive did not prove a satisfactory system for setting Defence Intelligence's priorities. In devising a new process, Defence Intelligence must take account of the results of the review of central intelligence structures and strategies, and the implications of that review for the setting of national priorities and tasking of the intelligence community.

U. The Committee welcomes the fact that Defence Intelligence is recruiting additional staff to expand its HUMINT capability, which is vital to counter the threat to our Armed Forces from Improvised Explosive Devices in particular. However, the Committee is concerned that the shortage of HUMINT instructors means that these new recruits cannot be deployed quickly. It is also concerning that existing HUMINT operators, who were already under pressure covering vacancies in theatre, are now being placed under further pressure by having to train the new recruits.

V. Defence Intelligence provides the largest single all-source assessment capability within the UK intelligence community. The ISC has, since 2008, consistently raised concerns about the diminution of its coverage and capability. The prospect of further

cuts – combined with the impact of cuts to BBC Monitoring, on which DI relies heavily – therefore has potentially very serious long-term consequences for DI's ability to support military operations and for the UK intelligence community as a whole.

W. The Committee welcomes the identification of cyber security as a Tier One risk in the National Security Strategy and the increased investment in this crucial area. However, concerns expressed in the ISC's last Annual Report concerning the lack of clear lines of responsibility and the potential risk of duplication of effort remain. The interests of national security demand that there should be clear lines of Ministerial accountability. We expressed concern that the original system was neither sensible nor appropriate. We strongly support the Government's decision to move Ministerial responsibility to the Cabinet Office.

X. The Government's decision to settle claims by former Guantánamo Bay detainees was unpalatable to many. Nevertheless, in the circumstances it was the most sensible course of action. The resources required to defend these claims would have been substantially greater than the cost of the settlement, but more importantly the damage that would have been done to foreign liaison relationships would have left the UK vulnerable. We therefore conclude that it was overwhelmingly in the public interest that the cases were settled out of court. We note that the Government continues to engage with US authorities to secure the release of Shaker Aamer, the last remaining former UK resident in Guantánamo Bay.

Y. The Committee welcomes the publication of the *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*. It is essential that the Government's overarching policy in relation to detainees, upon which the lower-level practical guidance used by the Agencies is based, is set out clearly and unambiguously.

Z. Whilst the previous Committee's *Review of the Government's draft guidance on handling detainees* has not been published, we note that the recommendations and conclusions made by the Committee in the last Parliament were taken into account by the current Government in considering the guidance and have been – to some extent – reflected in the final version now published by the Prime Minister.

AA. We agree with the Government that the Court of Appeal's decision in the Binyam Mohamed case, which resulted in a breach of the 'control principle', has raised serious concerns which need to be resolved urgently. We therefore welcome the Prime Minister's announcement of a Green Paper setting out how intelligence material might be protected in judicial proceedings. The Committee will respond to those proposals in due course.

BB. The Committee notes the Coroner's verdicts in the 7/7 Inquests, in particular that – as the ISC itself concluded in its 2009 Report – the Security Service and the police could not reasonably have prevented the attacks. The Committee supports the Coroner's recommendations that the Security Service should improve procedures for showing photographs to sources and that consideration be given to improving the recording of

decision-making in relation to the assessment of targets. We have asked the Security Service to report to the Committee on plans to address these matters and will report the progress made in our next Annual Report.

CC. We have identified eight examples where there were very minor inaccuracies or inconsistencies in evidence given to the ISC, compared with evidence subsequently provided to the Coroner. We have also identified three discrepancies which are more significant. These are extremely frustrating for the Committee, and for those who rely on our reports. We have satisfied ourselves, however, that they do not alter the conclusions and recommendations that were made in the Committee's *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*.

DD. The Coroner in the 7/7 Inquests acknowledged that the ISC's second report on the 7 July 2005 terrorist attacks was "*detailed and thorough*". However, she also noted the discrepancies between evidence to the ISC and that given to the Inquests, and criticised the Security Service for their poor record keeping. We share her concerns, having previously made the same point ourselves to the Agencies and to the two previous Prime Ministers. It is essential that the intelligence community make greater efforts to ensure that information provided to this Committee is full and accurate, that searches in response to Committee requests receive the same attention as requests from the courts, and that draft reports are reviewed properly, to ensure that such problems do not arise again.

EE. BBC Monitoring provides an irreplaceable service to the intelligence community, and offers considerable value for money due to the free flow of information with its far larger US counterpart. It is therefore of considerable concern to the Committee that its funding was arbitrarily cut without consultation in April 2010, in direct contravention of the governing Memorandum of Understanding, and that it now faces further cuts over the next two years. The Foreign Affairs Committee has already recommended revisiting the decision about the BBC World Service's funding, and we note the Government's decision to allocate an extra £2.2m to maintain Arabic services. There is also a powerful case for reviewing the decisions that were made about BBC Monitoring's funding in the 2010 Spending Review. The National Security Adviser must ensure that BBC Monitoring is able to maintain the level of service required by departments and Agencies. We strongly recommend that Ministers reconsider the cuts to BBC Monitoring in the period leading up to the transfer to licence fee funding.

FF. The Committee welcomes the greater emphasis now being put on collaborative working, both in terms of operational work and corporate services: the Agencies must explore all opportunities to make savings if they are to safeguard their core capability. They have made a good start and we encourage them to maintain this momentum.

GG. Although GCHQ has taken steps to reduce its vulnerability to disruptive events – for example through the planned closure of the less-resilient Oakley site – the Committee is very concerned that the lack of a back-up data centre leaves GCHQ exposed should its primary site be out of action. GCHQ should therefore bring forward specific proposals to address this risk at the earliest opportunity.

HH. The Committee accepts that there is a strong case for the Agencies to conduct vetting separately from other parts of government. However, there remains no convincing argument as to why each of the Agencies should maintain separate systems. A single organisation conducting vetting on behalf of all three, with the process tailored to each Agency's specific requirement, would offer considerable benefit. We recommend that the Agencies investigate this as both desirable in its own right and as a potential contribution to their savings targets during the 2010 Spending Review period, and await their response.

II. The Intelligence and Security Committee was established under the Intelligence Services Act 1994, and has now been in existence for over 16 years. We therefore considered that it was right to review whether the structure, remit and powers of the Committee were still sufficient in the context of the current intelligence machinery. It is clear that the current provisions are outdated and that the *status quo* is unsustainable. We have therefore submitted radical proposals for change that will ensure strengthened, more credible oversight of the UK intelligence and security Agencies and provide greater assurance to the public and to Parliament. We recommend that these form the basis for the proposals for reform of the ISC in the forthcoming Green paper on the handling of intelligence material in judicial proceedings.

JJ. Our proposals to the National Security Council are based on the following key principles:

- the Intelligence and Security Committee should become a Committee of Parliament, with the necessary safeguards, reporting both to Parliament and the Prime Minister;
- the remit of the Committee must reflect the fact that the ISC has for some years taken evidence from, and made recommendations regarding, the wider intelligence community, and not just SIS, GCHQ and the Security Service;
- the Committee's remit must reflect the fact that the Committee is not limited to examining policy, administration and finances, but encompasses all the work of the Agencies;
- the Committee must have the power to require information to be provided. Any power to withhold information should be held at Secretary of State level, and not by the Heads of the Agencies; and
- the Committee should have greater investigative and research resources at its disposal.

SECTION 9: GLOSSARY

BBCM	BBC Monitoring
BIS	Department for Business, Innovation and Skills
BME	Black and Minority Ethnic
CESG	Communications-Electronics Security Group
CDI	Chief of Defence Intelligence
CPNI	Centre for the Protection of National Infrastructure
CONTEST	UK Counter-Terrorism Strategy
CSR07	Comprehensive Spending Review 2007
CSOC	Cyber Security Operations Centre
DIGINT	Digital Intelligence
DI	Defence Intelligence
FATA	Federally-Administered Tribal Areas
FCO	Foreign and Commonwealth Office
GCHQ	Government Communications Headquarters
HFA	Hostile Foreign Activity
IA	Information Assurance
ICT	International Counter-Terrorism/Information and Communications Technology
IED	Improvised Explosive Device
INOC	Internet Operations Centre
ISC	Intelligence and Security Committee
IT	Information Technology
JIC	Joint Intelligence Committee

MoD	Ministry of Defence
NAO	National Audit Office
NDIST	Network Defence Intelligence and Security Team
NSA	National Security Adviser
NSC	National Security Council
OCS	Office of Cyber Security
OCSIA	Office of Cyber Security and Information Assurance
OGCIO	Office of the Government Chief Information Officer
OSCT	Office for Security and Counter-Terrorism
PFI	Private Finance Initiative
RIPA	Regulation of Investigatory Powers Act 2000
SDSR	Strategic Defence and Security Review
SIA	Single Intelligence Account
SIGINT	Signals Intelligence
SIGMOD	GCHQ's SIGINT Modernisation Programme
SIS	Secret Intelligence Service
SR10	Spending Review 2010

SECTION 10: LIST OF WITNESSES

Ministers

The Rt. Hon. Theresa May, MP – Home Secretary

The Rt. Hon. William Hague, MP – Foreign Secretary

The Rt. Hon. Baroness Neville-Jones – Minister for Security, Home Office (until May 2011)

Commissioners and Tribunal

The Rt. Hon. Sir Paul Kennedy – Interception of Communications Commissioner

The Rt. Hon. Sir Mark Waller – Intelligence Services Commissioner (from January 2011)

The Rt. Hon. Sir Peter Gibson – Intelligence Services Commissioner (until December 2010)

The Rt. Hon. Lord Justice Mummery – President, Investigatory Powers Tribunal

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Iain Lobban CB – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Sawers KCMG – Chief, SIS

Other officials

SECURITY SERVICE

Mr Jonathan Evans – Director General, Security Service

Other officials

DEFENCE INTELLIGENCE

Air Marshal Chris Nickols CB CBE – Chief of Defence Intelligence

Other officials

CABINET OFFICE

Sir Peter Ricketts GCMG – National Security Adviser

Mr Alex Allan – Chairman, Joint Intelligence Committee

Other officials

TSO
information & publishing solutions

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, telephone, fax and email
TSO
PO Box 29, Norwich NR3 1GN
Telephone orders/general enquiries: 0870 600 5522
Order through the Parliamentary Hotline Lo-Call: 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: www.bookshop.parliament.uk

TSO@Blackwell and other accredited agents

Customers can also order publications from
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
Telephone orders/general enquiries: 028 9023 8451
Fax orders: 028 9023 5401

ISBN 978-0-10-181142-2
9 780101 811422