Intelligence and Security Committee

Annual Report 2007–2008

Chairman:
Dr Kim Howells, MP

Intelligence and Security Committee

Annual Report 2007–2008

Chairman:

Dr Kim Howells, MP

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
by Command of Her Majesty
March 2009

Cm 7542 £14.35

From: The Chairman, Dr Kim Howells, MP

INTELLIGENCE AND SECURITY COMMITTEE

70 Whitehall, London SW1A 2AS

ISC 2008/09/064

16 December 2008

Rt. Hon. Gordon Brown, MP
Prime Minister
10 Downing Street
London
SW1A 2AA

Dear Gordon

I enclose the Intelligence and Security Committee's Annual Report for 2007–2008. This covers our work between December 2007, when we submitted our previous Annual Report, and November 2008.

The Committee has met on a total of 51 occasions during the reporting period, has taken oral and written evidence on the administration, policy and expenditure of the three intelligence and security Agencies, and has investigated related matters across the wider intelligence community. In addition to this Report, we have also produced a review of the links between the CREVICE plotters and the 7 July bombers, although it has not yet been possible to publish this.

We look forward to meeting you shortly to discuss our findings in detail, and would be grateful if the Report can be published as soon as possible thereafter.

Yours

Kim

KIM HOWELLS

THE INTELLIGENCE AND SECURITY COMMITTEE

Dr Kim Howells, MP (Chairman)[1]

The Rt. Hon. Michael Ancram QC, MP

The Rt. Hon. Sir Alan Beith, MP[2]

Mr Ben Chapman, MP

The Rt. Hon. Lord Foulkes of Cumnock

The Rt. Hon. George Howarth, MP

The Rt. Hon. Michael Mates, MP

Mr Richard Ottaway, MP

Ms Dari Taylor, MP

The Intelligence and Security Committee (ISC) was established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of the Security Service, Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ). The Committee has developed its oversight remit, with the Government's agreement, to include examination of intelligence and security-related areas within the Cabinet Office, including the Joint Intelligence Committee (JIC) and the Assessments Staff. The Committee also takes evidence from the Defence Intelligence Staff (DIS), part of the Ministry of Defence (MoD), which assists the Committee in respect of work within the Committee's remit.

The Prime Minister appoints the ISC members after considering nominations from Parliament and consulting with the leaders of the two main opposition parties. The Committee reports directly to the Prime Minister, and through him to Parliament, by the publication of the Committee's reports.

The members are subject to Section 1(1)(b) of the Official Secrets Act 1989 and have access to highly classified material in carrying out their duties. The Committee takes evidence from Cabinet Ministers and senior officials – all of which is used to formulate its reports. 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 (including original records, when relevant), or it may be memoranda specifically written for the Committee.

The Committee is required by the Intelligence Services Act to produce an Annual Report on the discharge of its functions, which the Prime Minister is required to lay before Parliament. The Committee can produce other reports on specific topics. When laying a report before Parliament, the Prime Minister can exclude any parts of the report (indicated by the *** in the text) that would be prejudicial to the continuing discharge of the functions of the three intelligence and security Agencies. This is done in consultation with the Committee. To date, no material has been excluded without the Committee's consent.

[1] *From 21 October 2008. The Rt. Hon. Margaret Beckett MP was Chairman of the Committee until 3 October 2008.*

[2] *Until 28 October 2008. At the time of writing, his replacement had not yet been appointed.*

CONTENTS

GLOSSARY

CESG	Communications-Electronics Security Group
CNI	Critical National Infrastructure
COBR	Cabinet Office Briefing Room
CONTEST	UK Counter-Terrorism Strategy
CPNI	Centre for the Protection of National Infrastructure
CSI	Ministerial Committee on the Security and Intelligence Services
CSR	Comprehensive Spending Review
DIS	Defence Intelligence Staff
DPBAC	Defence, Press and Broadcasting Advisory Committee
GCHQ	Government Communications Headquarters
HUMINT	Human-sourced Intelligence
IA	Information Assurance
ICG	Intelligence Collection Group
ICT	International Counter-Terrorism
ISC	Intelligence and Security Committee
IT	Information Technology
JARIC	Joint Air Reconnaissance Intelligence Centre
JIC	Joint Intelligence Committee
JTAC	Joint Terrorism Analysis Centre
MoD	Ministry of Defence
NAO	National Audit Office
NSID	Ministerial Committee on National Security, International Relations and Development
OSCT	Office for Security and Counter-Terrorism
PHIA	Professional Head of Intelligence Analysis
PSA	Public Service Agreement
PSNI	Police Service of Northern Ireland
R&Ps	Requirements and Priorities
RICU	Research, Information and Communications Unit
SFO	Serious Fraud Office
SIA	Single Intelligence Account
SIGINT	Signals Intelligence
SIGMOD	GCHQ's SIGINT Modernisation Programme
SIS	Secret Intelligence Service
SOCA	Serious Organised Crime Agency
SR	Spending Review

INTRODUCTION

1. This Report details the work of the Intelligence and Security Committee (ISC) for the period December 2007 to November 2008.

2. The Committee has held 26 formal sessions and 25 other meetings since we last reported in December 2007.[3] The attendance rate at these meetings has been over 90%.

3. During this time the Committee has primarily focused on its Review of the Intelligence on the London Terrorist Attacks on 7 July 2005.[4] This was a detailed investigation which took the Committee over 14 months to complete. We sent our findings to the Prime Minister in July 2008.

4. Whilst this Review was the Committee's top priority, during the year we have also examined and taken evidence on the policy, administration and expenditure of the three intelligence and security Agencies, and the wider intelligence community. We report on these matters here.

5. The Committee has undertaken a number of visits this year in relation to its work on the review of the intelligence on the 7 July bombings, including visits to the Security Service to examine material which was relevant to its Review. In addition, we have also visited the new Security Service facility in Loughside, Northern Ireland, the Police Service of Northern Ireland and the Government Communications Headquarters (GCHQ).

6. As part of the Committee's programme of discussions with our oversight counterparts, we have:

- attended the International Intelligence Review Agencies Conference, held in New Zealand;
- held bilateral discussions with our Australian counterparts and the Australian intelligence agencies;
- attended the Conference of the Parliamentary Committees for the oversight of intelligence and security services within the European Union, held in Portugal;[5] and
- hosted visitors from Australia, Canada, Romania, Singapore and the United States.

7. On 24 January 2008, the Committee's Chairman, the Rt. Hon. Paul Murphy MP, was appointed Secretary of State for Wales. The Prime Minister appointed the Rt. Hon. Margaret Beckett MP as the new Chairman of the Committee on 29 January. The Committee wishes to express its appreciation to Mr Murphy for his chairmanship since July 2005.

[3] *As at 7 November 2008.*

[4] *On 30 April 2007, the Prime Minister asked the Committee to reappraise the matters and questions it had examined in its original report into the 7 July attacks, in light of evidence arising from the CREVICE fertiliser bomb plot trial.*

[5] *The Chairman attended this conference on behalf of the Committee.*

8. On 3 October 2008, the Prime Minister appointed the Rt. Hon. Margaret Beckett MP as Minister of State for Housing and Planning. The Committee wishes to record its thanks to Mrs Beckett for her leadership during this year. The Prime Minister appointed Dr Kim Howells MP as the new Chairman of the Committee on 21 October 2008.

Reform of the Intelligence and Security Committee

9. The Government published *The Governance of Britain* Green Paper in July 2007.[6] It contained suggestions for reform of this Committee and invited the Chairman to:

> *… advise on how to maximise the effectiveness of the Committee's scrutiny role, including on the Committee's relationship to Parliament and to relevant Select Committees, under the existing legislation.*

10. The Committee submitted a memorandum to the Prime Minister in October 2007 containing detailed proposals, designed to increase public knowledge and awareness of the Committee's work and to strengthen the Committee's relationship with Parliament, but equally importantly to provide stronger, more effective oversight of the UK intelligence and security Agencies.

11. The Prime Minister announced plans for reform of the Committee on 19 March 2008. In a statement to the House of Commons he said:

> *We will go ahead to introduce a resolution of both Houses – in advance of any future legislation – that will enshrine an enhanced scrutiny and public role for the Intelligence and Security Committee. This will lead to more Parliamentary debate on security matters, public hearings on the National Security Strategy, and – as promised – greater transparency over appointments to the Committee so that the Committee can not only review intelligence and security but also perform a public role – more akin to the practice of Select Committees – in reporting to and informing the country on security matters.*[7]

12. The White Paper *The Governance of Britain – Constitutional Renewal*,[8] published on 25 March, listed the proposed reforms in detail:

- *to amend the appointments procedure to enable the full participation of Parliament, by adopting a process similar to that for joint Select Committee appointments, which sees nominations for membership being sent to the Prime Minister who would make the final appointments in consultation with the Leader of the Opposition;*
- *the [Government] to provide public briefings [to the Committee] where this can be achieved without compromising national security or the safety of individuals;*
- *an investigator post… to be revived with consideration to be given to a pool of individuals with different expertise on whom the Committee could call;*

[6] *Cm 7170.*

[7] *HC Deb 19 March 2008 vol 473 c 926.*

[8] *Cm 7342.*

- *to emphasise the Committee's independence… [the Government] will explore alternative accommodation options;*
- *in future, debates should also take place in the House of Lords; and*
- *ISC debates [should be] opened by the Chair of the Committee. Lords debates should be opened by the senior Lords Committee member.*

13. On 17 July 2008 the following resolution was passed in the House of Commons:

> *That this House endorses the proposals for the reform of practice and operation of the Intelligence and Security Committee as set out in paragraphs 235–244 of* The Governance of Britain *White Paper Cm 7342-1, including provision for nomination of the members of the Committee drawn from the House of Commons to be based in future on proposals made by this House.*

The following Standing Order was also passed:

> *The Committee of Selection may propose that certain members be recommended to the Prime Minister for appointment to the Intelligence and Security Committee under section 10 of the Intelligence Services Act 1994.*

On 13 November 2008, the House of Lords approved the proposed arrangements for nominating the Lords membership of the Committee and increasing the House of Lords' scrutiny of its work.

14. The Committee welcomes the reforms proposed by the Prime Minister and endorsed by Parliament, subject to the necessary resources being made available by the Cabinet Office. During the debate in the House of Commons, the Foreign Secretary said:

> *It is in our interest… that scrutiny is as rigorous as possible given the limits that need to exist… we are committed to ensuring that the Committee has what it needs to carry out its duties effectively.*[9]

15. In addition to the reforms outlined in the White Paper and agreed by Parliament, one of the issues that the Committee has itself kept under review is that of access to documents. Although the Intelligence Services Act 1994[10] includes provisions which restrict the disclosure of sensitive information to the Committee, in practice the Committee has been afforded access to highly sensitive and operational information and there has been only one instance where the Committee has been denied sight of specific documents.[11] With this one exception, the Committee's access to documents has been supported by successive Prime Ministers, including the current Prime Minister. At the start of our recent Review of the Intelligence on the London Terrorist Attacks on 7 July 2005 the then Prime Minister specifically asked that the Committee be able to see all the material necessary. Such flexibility has proved essential in allowing the Committee to carry out its

[9] *HC Deb 17 July 2008 vol 479 cc 495–497.*

[10] *The Intelligence Services Act 1994 established the Intelligence and Security Committee.*

[11] *This issue was covered in our 2006–2007 Annual Report (Cm 7299).*

oversight remit effectively. In a number of instances this has brought important information to the attention of Ministers or senior officials about which they would otherwise have been unaware. Access to such information and documentation should be maintained in the future.

16. In terms of the Committee's remit, the Intelligence Services Act 1994 established the scope of the Committee's oversight responsibilities – to examine the expenditure, administration and policy of the Security Service, the Secret Intelligence Service (SIS) and GCHQ. As the content of this Report shows, however, the work of this Committee is, in practice, much broader than this. The Committee has for many years taken evidence from the Chief of Defence Intelligence on aspects of the work of the Defence Intelligence Staff, and also from the Cabinet Secretary, the Joint Intelligence Committee Chairman and senior Cabinet Office officials on the national intelligence machinery.[12]

A. The work of the intelligence and security Agencies cannot be looked at in isolation and it remains essential that this Committee has oversight of the wider intelligence community.

[12] *Where relevant to the ISC's remit under the 1994 Act (for example, following the loss of two Joint Intelligence Committee papers in June 2008, Sir David Omand was asked to undertake a review of the incident and keep this Committee fully informed. This matter is covered in paragraphs 177 to 182).*

THE AGENCIES

The threat

17. There continues to be a wide range of threats to the UK, both terrorist and non-terrorist. The Government's National Security Strategy outlines the breadth of those threats.[13]

18. The current threat to the UK from international terrorism is assessed as "Severe".[14] This means that there is a continuing high level of threat to the UK and, in particular, that there is a high likelihood of a terrorist attack in this country. The threat has not fallen below this level since July 2005, and has been described as *"on a scale not previously encountered"*.[15]

19. The threat of international terrorism comes from a diverse range of sources, including al-Qaeda and associated networks, and those who share its ideology but who do not have direct contact with them. Al-Qaeda and related terrorist groups have shown an exceptional level of ambition and willingness to carry out indiscriminate terrorist attacks, and the threat they pose is likely to persist for a considerable time. This places considerable pressure on the intelligence and security agencies – working with the police, government departments and other key partners – which are working to find those who are planning an attack and prevent them from carrying it out.

20. As at the end of September 2008, the Security Service was undertaking approximately *** major investigations, of which around *** represented a high level of threat. So far in 2008, 46 people have been convicted in 15 significant terrorism cases.

21. Whilst the primary focus is necessarily on international counter-terrorism (ICT) work, the UK's intelligence and security Agencies also dedicate resources towards countering the challenges posed by ***, ***, the proliferation of weapons of mass destruction, regional instability in *** and the ***, and other challenges. In addition, they continue to provide unprecedented operational support to UK military operations.

22. The Agencies' resources have increased, and indeed will continue to increase over the next three years, but they still have to make difficult decisions about priorities, often on a daily basis. The stark reality is that they cannot cover all the threats to the level they would wish.

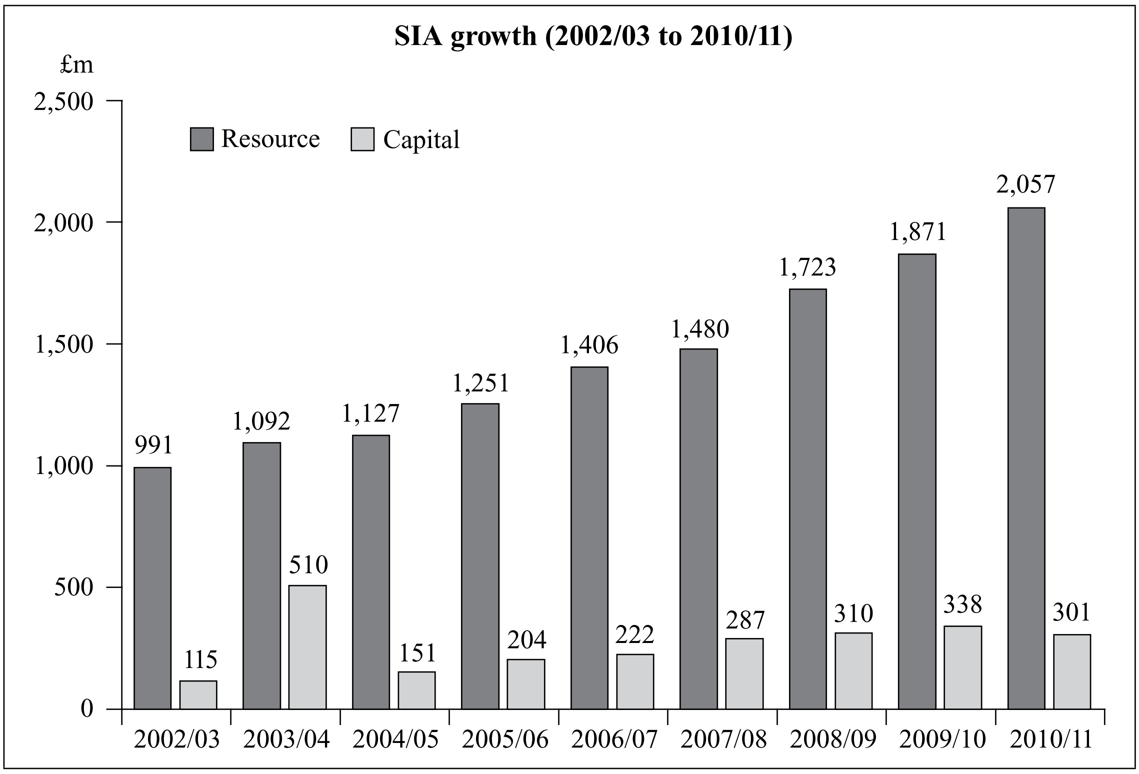
[13] *The key security challenges to the UK, as outlined in the National Security Strategy (published in March 2008), are listed in paragraph 122.*

[14] *As at 7 November 2008.*

[15] *www.cpni.gov.uk, 12 November 2008.*

The Single Intelligence Account

23. In October 2007, the Government published the outcome of its Comprehensive Spending Review 2007 (CSR07). As we noted in our 2006–2007 Annual Report, this included a settlement for the Single Intelligence Account (SIA) which increased the funding available for the intelligence and security Agencies to just over £2 billion by 2010/11. The chart below shows the growth in SIA[16] funding since 2002/03.



24. At the time of our last report, the overall SIA settlement had not yet been divided between the Agencies. In this Report, we outline the allocation of the additional funding between the Agencies, their spending priorities, and their expenditure plans for this additional money.

[16] *The SIA expenditure figures set out here, and all SIA-related data provided below, are derived from the audited and published SIA Consolidated Accounts and GCHQ, SIS and Security Service accounts for each financial year. Data indicates actual/planned SIA expenditure totals for the period 2002/03 to 2010/11.*

25. The following table shows the actual and planned expenditure for the period 2005/06 to 2010/11.[17]

£ million		**Actual 2005/06**	**Actual 2006/07**	**Actual 2007/08**	**Planned 2008/09**	**Planned 2009/10**	**Planned 2010/11**
SIA total[18]	**Resource**	**1,251.2**	**1,405.5**	**1,479.9**	**1,722.5**	**1,870.5**	**2,056.5**
	Capital[19]	**204.1**	**221.8**	**286.6**	**309.7**	**338.0**	**301.0**
GCHQ[20]	Resource	***	***	***	***	***	***
	Capital	***	***	***	***	***	***
SIS	Resource[21]	***	***	***	***	***	***
	Capital	***	***	***	***	***	***
Security Service	Resource	***	***	***	***	***	***
	Capital	***	***	***	***	***	***
Additional elements[22]	Resource	***	***	***	***	***	***
	Capital	***	***	***	***	***	***

26. As the table above shows, the CSR07 provides the Agencies with an additional £265.7 million for 2008/09, £176.3 million for 2009/10, and £149.0 million for 2010/11. Much of this funding is needed to consolidate the increases in the Agencies' budgets since the baseline was last set as part of SR2004 – in other words, to maintain the Agencies' capabilities at current levels. This means:

- for GCHQ, 78% of the additional £*** million it received will be used to consolidate its current position, with 22% available for further expansion and additional investment in new capabilities;
- for the Security Service, 20% of the additional £*** million it received will be used to consolidate its current position, with 80% available for expansion and investment in new capabilities; and

[17] *The Committee considers in detail the approved accounts for the Agencies. Due to the timing of the Annual Report, the Report comments on the previous year's accounts. Therefore, for this 2007–2008 Annual Report, the detail is given on the 2006/07 accounts. The table shows actual expenditure up to 2007/08 and planned budgets for 2008/09, 2009/10 and 2010/11 (including the CSR07 settlement).*

[18] *SIA totals for each financial year combine resource and capital expenditure figures for GCHQ, SIS, the Security Service and additional elements.*

[19] *The capital figures refer to net cash expenditure on fixed assets for 2005/06. Since 2006/07, capital expenditure has been taken on an accruals basis.*

[20] *This takes account of the GCHQ to Ministry of Defence (MoD) Public Expenditure Survey Transfer of £*** million per annum with effect from 2007/08. The figures include National Technical Assistance Centre budgets with effect from 2006/07 (totalling £*** million).*

[21] *The SIS resource figures from 2008/09 inclusive will be reduced each year by a £*** million baseline transfer to the Serious Organised Crime Agency (SOCA).*

[22] *The 2005–2006 Annual Report included a SIA "level adjustment" – an end of year accounting adjustment on consolidation for 2005/06 and preceding financial years. Figures indicated above for 2005/06, 2006/07 and 2007/08 are SIA additional elements that include accounting adjustments on consolidation and the ***. ***. From 2008/09 onwards, figures indicate funding elements including SCOPE and Information Assurance. Accounting adjustments on consolidation mean that the figures above do not replicate the audited accounts for the Agencies in every case.*

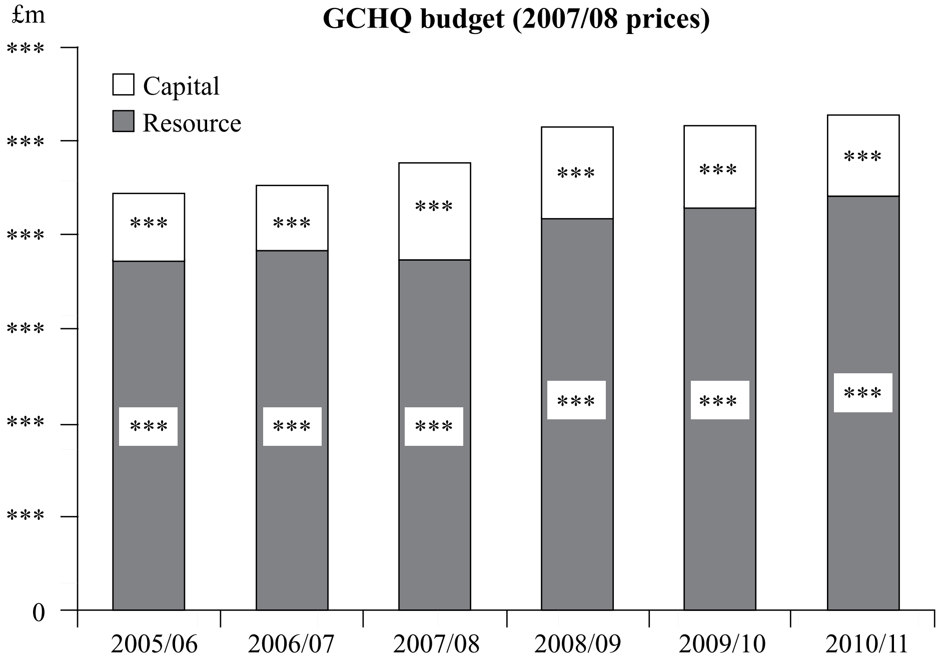
- for SIS, 31% of the additional £*** million it received will be used to consolidate its current position, with 69% available for expansion and investment in new capabilities.

27. The breakdown of how the Agencies will each allocate their additional resources is contained in the individual sections below. These are listed below by size of budget.

Government Communications Headquarters

Expenditure

28. The following chart demonstrates the growth in GCHQ's spending.[23]



29. GCHQ's net operating costs rose to £*** million for 2006/07 – an increase of 5.8% from 2005/06.[24] GCHQ's budget for 2007/08 was £*** million.

30. The CSR07 settlement gave GCHQ a budget of £*** million for 2008/09 rising to £*** million for 2010/11. The additional money from CSR07 will be used as follows:

- increasing GCHQ's counter-terrorism effort – primarily operational support in the UK to an expanding Security Service, but also work against strategic international terrorism-related targets;
- further growth in capability to combat extremist use of the internet in the UK and abroad; and
- improving internet-related capabilities.

[23] *These figures show spending in 2007/08 prices calculated on the basis of the latest HM Treasury deflators (as at 30 September 2008). The same deflators have been applied to the figures in the charts at paragraphs 45 and 72.*

[24] *GCHQ's Resource Account was agreed by the Comptroller and Auditor General in July 2007.*

31. One of the heaviest demands on GCHQ's budget relates to its technology improvement programme. As we have reported in previous years, GCHQ runs a number of major technical projects designed to maintain and enhance its signals intelligence (SIGINT) capabilities – collectively these projects form the SIGINT Modernisation (SIGMOD) programme.[25] The programme for the next three years alone is expected to cost £*** million (both resource and capital expenditure), and is expected to continue at a similar rate of spending for the foreseeable future. The major projects within the programme at this time are listed below:

- IT infrastructure – this will cost £*** million over the next three years and covers investment and maintenance of GCHQ's IT backbone, which underpins the rest of the modernisation programme.
- Internet programme – costing £*** million over the next three years, this project includes a number of elements which together are designed to enable GCHQ to keep up with the rapid progression of internet technologies. The project aims to improve the identification, interception and management of internet-based communications.[26]
- "Better Analysis" – the aim of this project is to improve the use of the intelligence material that GCHQ collects, including with foreign liaison partners. It has a budget of £*** million over the next three years.
- Support to military operations – providing SIGINT support to military operations is one of GCHQ's core functions. This project will improve technical coverage and capabilities specifically in areas where UK military forces are deployed and aims to support and enhance the effectiveness of UK forces overseas. GCHQ plans to spend £*** million over the next three years on support to military operations.

32. The funding required by SIGMOD is considerable and represents a significant proportion of the SIA budget. Whilst some of the work involves the enhancement of current capabilities, a small number of projects involve the development of new and anticipatory capabilities. Inevitably, some of these carry an element of financial risk. The Committee recognises, however, that investment in SIGMOD is essential if GCHQ is to keep up with the rate and complexity of technological change.

Policy

International counter-terrorism

33. GCHQ reviewed its counter-terrorism strategy in 2007, resulting in the following priorities:

[25] *Signals intelligence (or SIGINT) is intelligence derived from GCHQ's statutory requirement (under the Intelligence Services Act 1994) to "… monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material".*

[26] *One of the most significant challenges facing GCHQ is to maintain its capability to identify and intercept targets as communications – including telephony – increasingly move to Internet Protocol technology. This challenge is faced on a broader scale across the intelligence and law enforcement communities and the Home Office is therefore co-ordinating the Interception Modernisation Programme to address the challenge. This is covered in paragraphs 174 to 176.*

- greater emphasis on strategic reporting;
- more focus on terrorist use of the internet; and
- improving the co-ordination of PREVENT work.

34. GCHQ devoted around a third of its total effort to counter-terrorism during 2006/07 with a small increase planned in 2007/08.[27]

35. Of GCHQ's total ICT effort, ***% was in support of Security Service operations and this continues to be a growing demand on, and a challenge for, GCHQ.[28] GCHQ has agreed performance targets with the Security Service for the level of support it will provide to operations; however, the Director of GCHQ told the Committee that these are extremely difficult to meet:

> *We don't quite meet the targets they set, but, frankly, the targets they set are at a level where it is very unlikely we ever would be able to meet them… I think their aspirations would almost always exceed our capability.*[29]

36. A further ***% of GCHQ's ICT effort is on what it calls "strategic reporting" – long-term assessments of the way terrorists operate. The Director of GCHQ used *** as an example of this work:

> *We look at the *** for example, so we can identify some of the ****
> **** … We are looking to see what these ****
> ****.*[30]

37. The remaining ***% of GCHQ's ICT effort is on a range of issues, including:

- research to understand how terrorists are using the internet;
- work on the potential cyber-terrorist threat;
- research into the ICT ***; and
- helping other countries to build their ICT capacity.

Non-ICT work

38. In addition to the expansion of effort on ICT work, GCHQ is increasing effort on other priorities, including work to counter electronic attacks against UK networks, on strategic political and economic issues, energy security and nuclear proliferation.

[27] *Although it should be noted that other parts of GCHQ's work, some of which absorb considerable resources (such as SIGMOD), will indirectly, or in the longer term, benefit its work on ICT.*

[28] *We considered this in our Annual Report last year (Cm 7299).*

[29] *Oral evidence – GCHQ, 19 February 2008.*

[30] *Oral evidence – GCHQ, 19 February 2008.*

39. Demand for GCHQ support to UK military operations has also continued to increase, particularly in Afghanistan. To address these demands, GCHQ has established a specialist team of staff who are selected and trained for deployment overseas in support of UK military operations. It has also increased the use of SIGINT to identify and locate terrorist suspects, in support of operations by both regular and special forces. GCHQ plans to spend £*** million over the next three years on developing its technical capability further to support military operations overseas.

40. Another growing demand on GCHQ is the provision of Information Assurance (IA) services.[31] GCHQ, via the Communications-Electronics Security Group (CESG), offers IA services to a large number of customers (including central and local government, the UK military, critical national infrastructure companies and other companies).[32] GCHQ had already planned to expand this work, anticipating a growth in demand; however, these plans were accelerated following the loss of personal data by Her Majesty's Revenue and Customs in November 2007 which resulted in an increased demand for CESG services. The Director of GCHQ told us:

> *… people are now biting my hand off for support… The challenge now is how do we provide this much support in the volume that people want it and as quickly as they want it. It is a good problem to have, but it is not, in the very short term, particularly easy.*[33]

41. GCHQ is adapting its organisational and management structures to meet the challenge of growing demand for IA, both now and in the longer term.[34] ***
***.
***.[35] ***
***.
GCHQ is retaining the current external branding of its services, since CESG is a well established organisation that has supported clients in both the public and private sectors for many years.

Administration

42. GCHQ recruited over 350 staff during 2006/07 (90% of its target) and plans to recruit around 1,250 staff over the next three years. As a result of GCHQ's long-running problems in recruiting and retaining specialists (including linguists, analysts, technologists and internet/network experts), GCHQ introduced a new recruitment and retention payment policy in 2007, which was designed to ensure that it pays the market rate for specialist posts.

[31] *Information Assurance involves offering advice and assistance to keep critical communication and information systems secure from a variety of threats and disruption (for example hackers, criminal gangs seeking sensitive information, and terrorists attempting to find vulnerabilities in the delivery of critical services).*

[32] *CESG is the National Technical Authority for Information Assurance.*

[33] *Oral evidence – GCHQ, 19 February 2008.*

[34] *As part of this organisational change, GCHQ has created a new Director General-level post responsible for Information Assurance and technology. This will allow senior staff to focus more on external Information Assurance customers, and the challenges and opportunities of new technology.*

[35] *This relates to GCHQ's various activities ***.*

43. The Director of GCHQ told us that although overall resignation rates have now dropped back to acceptable levels, he remained concerned about retention in some of the specialist groups, particularly experienced technologists and internet/network experts, and the impact of this on some of GCHQ's development work:

> *Our graduate recruitment salaries are reasonably competitive but we lose traction in mid career. So after people have been with us a few years they are earning less than they could have earned if they were working in the outside world… There is a tendency now to lose people at the… five to eight year point… They have got a lot of experience and they are really quite valuable.*[36]

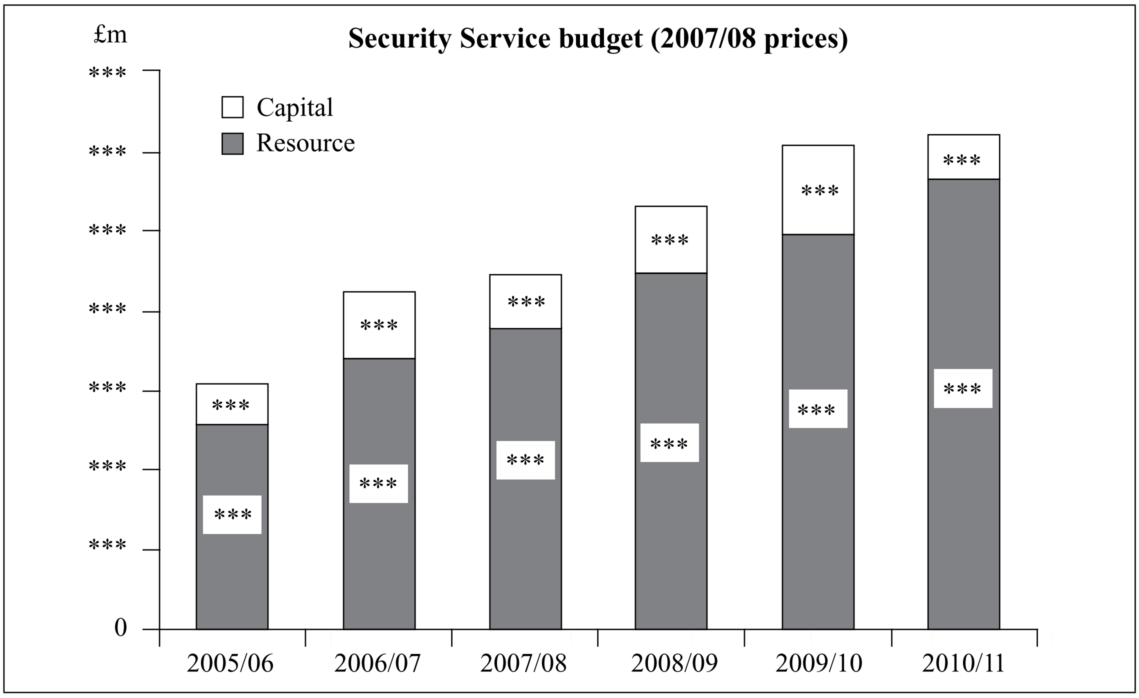
B. We appreciate the challenge involved in retaining highly trained and specialist staff over the long term, and are encouraged by the steps that GCHQ has taken so far to deal with this problem.

44. In July 2008, Sir David Pepper retired as Director of GCHQ after five years in post. Sir David has presided over the organisation during a period of unprecedented challenge and change, and the Committee wishes to take this opportunity to praise his leadership and commitment over this period. Iain Lobban succeeded Sir David as Director at the end of July 2008.

The Security Service

Expenditure

45. The following chart demonstrates the growth in the Security Service's spending.[37]



[36] *Oral evidence – GCHQ, 19 February 2008.*

[37] *These figures show spending in 2007/08 prices calculated on the basis of the latest HM Treasury deflators (as at 30 September 2008). From 2007/08, the Security Service figures exclude downward fixed asset price movements which are charged to Annually Managed Expenditure – £*** million in 2007/08.*

46. Security Service spending during 2006/07 rose by almost 41% to around £*** million (from £*** million the previous year).[38]

47. Capital spending in 2006/07 rose to £*** million (an increase of nearly 70% over 2005/06). This money was spent on major technical and accommodation projects, including:

- £*** million on a Northern Operations Centre;[39]
- £*** million on the Service's new building in Northern Ireland;[40]
- £*** million on a new secure communications system;
- £*** million on a technical garage and repair facility; and
- £*** million for a covert intelligence distribution system.

48. In the CSR07, recognising the sustained threat from international terrorism, the Government committed significant additional resources over the next three years to enable the Security Service to deliver improved assurance against the possibility of terrorist attack. The Service has identified four front-line operational priority areas for strategic investment over the three-year period:

i. the "IQ Programme" – using technology to double investigative capacity by improving the processing and exploitation of intelligence;[41]

ii. increasing transcription capability to meet demand;

iii. increasing the impact and improving the effectiveness of the Service's agent-running capability;[42] and

iv. increasing the Service's regional presence to reinforce its partnership with the police.

These four priorities will be underpinned by strategic investment in the following areas:

i. improving and enhancing core IT;

ii. investing in training and development of present and future staff;[43] and

iii. creating space to accommodate planned staff growth within existing buildings.

[38] *The Security Service Resource Account for 2006/07 was agreed by the Comptroller and Auditor General in October 2007.*

[39] *See paragraph 54.*

[40] *See paragraph 56.*

[41] *See paragraph 52.*

[42] *The Service aimed to do this by increasing operational staff numbers (in 2001 the Security Service had *** agent handlers working against the ICT target – this has increased to *** currently and over the next three years will grow further), improving training of agent handlers and appointing a Head of Profession for operational officers to encourage best practice.*

[43] *This includes the launch of a Management Development Gateway in October 2008, giving managers the opportunity to build on existing leadership skills; the development of an e-learning capability, reaching regional staff and shift working staff more easily; and training on responding to critical incidents such as terrorist attacks.*

49. The Security Service programme of future major projects over the next three years includes £*** million for the first tranche of the "IQ Programme" and £*** million for accommodation to house the Service's corporate services.

Policy

International counter-terrorism

50. In 2006/07, the Security Service allocated 63% of its resources to ICT (an increase of 10% on the previous year). In 2007/08 the Security Service allocated 67% of its resources to ICT (£*** million).

51. Whilst the Security Service continues to deploy resources on discovering new potential terrorist networks and plots, it is increasingly finding that intelligence about extremist activity relates to individuals who have already surfaced on some level in previous investigations. The Director General told the Committee:

> *[One of our priorities is] to try and know more about the people we already know about, rather than to find the people we don't know anything about. It would be nice to know about the unknown unknowns, but it is probably a less rich seam than knowing more about the people that we know are a threat to us.*[44]

This means that the Service is focusing its efforts on making better use of the intelligence already at its disposal – it needs to innovate to improve the methods by which it collects, analyses and acts upon intelligence.

52. The Service completed the first phase of its "Information Exploitation (IE) Programme" in June 2007 at a cost of £*** million. The programme provides tools to enable investigators to search across systems, map networks and analyse events based on time and geography. It therefore allows specialist analysts to focus on more complex, in-depth analysis. The second phase, when completed, will double investigative capability by transforming the Service's ability to process and exploit intelligence. It will improve the way investigators are able to use intelligence from a variety of sources, and provide what the Director General has described as "trip-wire" coverage of significant patterns of activity. It will also allow staff to bring the intelligence together and analyse it more effectively. This second phase has now been incorporated into the "IQ Programme".[45]

53. The Service's network of regional stations continues to develop, with nine now established, giving them a nationwide presence. It is expected that by 2011 around 25% of Service staff will work outside Thames House. One of the real advantages has been the better use being made of the police's counter-terrorism capabilities through a combination of technological improvements and closer joint working. The regional offices also enhance the relationship between the Service and local police Special Branches, which are crucial to the successful running of joint counter-terrorism operations. An additional benefit has

[44] *Oral evidence – Security Service, 25 March 2008.*

[45] *The "IQ Programme" is scheduled over the CSR07 period and beyond. It aims to build on the "IE Programme" by providing investigators with context and connections to what they already know about their targets, saving time on searches. The first part of the "IQ Programme" is scheduled to go live in 2009/10.*

been an improvement in the Service's ability to gather and assess local intelligence. This is being supported by a new range of IT capabilities to manage nationally growing numbers of agents and to ensure consistent intelligence reporting into joint investigations.

54. A very real practical benefit of the regionalisation programme is the ability to respond to events across the UK more quickly than before. The Director General explained:

> *If one takes, for an example, the events of the London/Glasgow attacks in June [2007]… if we had… forward mounted some of the equipment and surveillance in the north ***, our response would have been considerably quicker in getting up to Scotland, particularly some of the equipment because we had to find some way of getting the stuff up to Glasgow. You would be starting two-thirds of the way there, which would in fact have been considerably advantageous to us…*[46]

The Security Service recently opened a Northern Operations Centre to provide an operational support capability from a base outside London. This is particularly beneficial given the UK-wide nature of the threat that the Service is trying to cover.

Non-ICT work

55. The threat from Irish-related terrorism has diminished in recent years – the Independent Monitoring Commission reported, in November 2007, that the Provisional Irish Republican Army is fully committed to the political process. However, dissident republican groups such as the Real IRA and Continuity IRA are opposed to the current process and continue to pose a threat to Great Britain, and to Northern Ireland in particular. Some loyalist groups continue to engage in violence and other forms of serious crime. The Security Service therefore allocated 17% of its resources to Irish-related terrorism in 2006/07, with 15% allocated for 2007/08.

56. We reported last year that the Security Service had completed building its headquarters in Northern Ireland, having taken lead responsibility for national security there in October 2007, and that the new headquarters provide the Service with much-needed additional accommodation. Having a base in Northern Ireland also facilitates the Service's relationships with other organisations in Northern Ireland, including the Police Service of Northern Ireland (PSNI). There are ***
***. The station provides the Service with invaluable capability and flexibility to respond to the ever-changing threat picture, from both Irish-related threats and international terrorism, and also provides an important back-up facility for the Service.[47]

57. The Committee visited the new headquarters in December last year and also met Sir Hugh Orde, the Chief Constable of the PSNI. The two organisations continue to work closely on collection and assessment work.

[46] *Oral evidence – Security Service, 25 March 2008.*

[47] *We discuss the Service's business continuity arrangements in paragraphs 96 to 98.*

58. During our visit, the Chief Constable explained that one of the greatest burdens placed on his police force is the increasing number of retrospective investigations, inquests and inquiries being conducted (of which, by the end of 2008, there were nearly 3,000). Each case requires access to vast amounts of archive information and they were proving prohibitively resource-intensive for the police. The House of Commons Northern Ireland Affairs Select Committee expressed similar concerns in its report *Policing and Criminal Justice in Northern Ireland: the Cost of Policing the Past*, published in June 2008:

> *The statutory inquiries place significant demands on the PSNI at a time when police officers are still subject to attacks from dissident terrorists. No other police force in the United Kingdom is required to operate in such an environment, and at the same time to service the demands of the extensive range of historic investigations which are underway in Northern Ireland.*[48]

59. Another key non-ICT focus for the Service is its counter-espionage work. The Security Service dedicates 3.5% of its resources to such work, with particular focus on China and Russia.

60. The murder of the Russian dissident Alexander Litvinenko in London in November 2006 led to a serious deterioration in diplomatic and political relations between Russia and the UK.[49] In response to the Litvinenko murder, the Security Service increased its resource dedicated to Russia by around ***%. The Director General told the Committee that:

> ***
> ***
> ***.[50]

This focus on Russia is something the Director General has commented on publicly:

> *Since the end of the Cold War we have seen no decrease in the numbers of undeclared Russian intelligence officers in the UK… conducting covert activity in this country… [The Security] Service is still expending resource to defend the UK against unreconstructed attempts by Russia… and others, to spy on us… It is a matter of some disappointment to me that I still have to devote significant amounts of equipment, money and staff to countering this threat.*[51]

61. The Director General told the Committee that resource limitations mean that, at present, "***" remains the Security Service's objective.[52]

[48] *HC 333.*

[49] *Just before his death, Litvinenko accused the Russian Government of involvement in his murder. In May 2007, the UK requested Russia's agreement for the extradition of the chief suspect Andrei Lugovoi. Following Russia's refusal, the Foreign Secretary announced in Parliament on 16 July 2007 the expulsion of four Russian diplomats from the UK. The Russian Government responded by expelling four British diplomats from Russia, and stepped up measures against the British Council operating in Russia, including threats to close down its operations outside Moscow, and the intimidation of local staff employed by the British Council. The British Council offices in St Petersburg and Ekaterinburg were prevented from operating and, therefore, it decided to suspend its operations in the two cities.*

[50] *Oral evidence – Security Service, 25 March 2008.*

[51] *Speech by the Director General of the Security Service to the Society of Editors – "Intelligence, counter-terrorism and trust", 5 November 2007.*

[52] *Oral evidence – Security Service, 24 January 2008.*

Protective security work

62. The Service continues to devote significant effort to protective security work through its contribution to the Centre for the Protection of National Infrastructure (CPNI).[53] Although the proportion of the Security Service's effort on protective security has fallen (from 14% in 2005/06 to 10% in 2006/07), it has actually been able to spend more because of the rise in its overall budget. This has been vital in light of the growing demand for CPNI advice.

Administration

Staffing

63. The Security Service has continued its rapid recruitment programme and by April 2008 had a total of 3,382 staff (including secondments and attachments). Staff numbers are projected to grow still further – to around 4,100 by 2011.

64. The recent recruitment has been largely at junior levels, with year-on-year growth of around 30% in these grades since April 2006. This has boosted the number of front-line staff involved directly in counter-terrorism work – co-ordinating investigations, running agents and conducting surveillance against targets – and will provide the Service with the physical capacity to investigate and cover more of the terrorist threat.

65. To achieve its recruitment targets, the Service has had to streamline its recruitment processes to enable it to sift a large number of candidates quickly and effectively. This has also helped the Service to fulfil its growing requirement for specialist and niche roles.

66. The Security Service has established an "Ethical Counsellor" post[54] to provide staff with an internal avenue to raise any ethical concerns they may have about the Service's work with someone who is outside their management line.[55] Around 12 individuals have been to see the Ethical Counsellor since 2006.[56]

C. It is reassuring that so few Security Service staff have felt the need to raise ethical concerns or complaints with the "Ethical Counsellor". We nevertheless welcome the establishment of the post and believe it provides an important avenue, should the need arise, for staff to discuss their concerns.

[53] *CPNI is discussed in detail in paragraph 138.*

[54] *The "Ethical Counsellor" post is a senior post currently held by a former Deputy Director General of the Service.*

[55] *In the absence of an equivalent post within SIS or GCHQ, staff working in those Agencies are advised that they have access to the Staff Counsellor, an externally appointed independent senior figure available to all members of the intelligence and security services. The Staff Counsellor can be consulted in confidence by any member of staff with anxieties relating to the work of their service.*

[56] *The concerns the individuals have raised include: whether the Service had adequate mechanisms to evaluate the mental and physical health risks to ICT agents; whether the Service should be involved in PREVENT work given the pressure it faces to tackle the terrorist threat directly; whether it was ethical for the Government to seek to alter the ideological views of its citizens (as part of its counter-radicalisation strategy); and whether there were sufficient controls for sharing information with countries that do not comply with international standards for the treatment of those in detention and whether guidance for staff on these matters was sufficiently accessible and understood.*

Vetting

67. In April 2008 it emerged that one of the women involved in the exposé relating to Max Mosley (President of the Fédération Internationale de l'Automobile) was the partner of a member of the Security Service. The member of staff was immediately suspended from the Service since he had failed to inform the Service about what he knew. He has now resigned.

68. The Security Service instigated an internal review of its vetting arrangements relating to this incident and reported its findings to this Committee. We were told that, as part of continuous personnel security management (vetting), checks are carried out on spouses or partners of staff (although they do not receive the same level of scrutiny as the member of staff) and this information has a direct bearing on the decision as to whether or not to reaffirm an individual's security clearance. Critically, despite the rigorous nature of the checks carried out, the process nevertheless relies on individuals being open and honest and informing the Service about their personal circumstances – something this member of staff singularly failed to do. The Director General told the Committee that the key lesson the Service has learnt from the incident is the need to underline more clearly to staff their responsibility to report any changes in their personal circumstances, so that the Service can assess any potential security risks.

69. This incident has highlighted the risks inherent in the vetting system used by all three Agencies. The Committee intends to look at this in more detail in the near future.

Consultants

70. The Security Service employs approximately 350 consultants. Of these, around 160 are filling support roles to allow Service staff to be redeployed to front-line work. The Service aims to use the CSR07 settlement to reduce its current dependency on contractors and, as a result, it should benefit from cost savings in the long term. The Committee welcomes this commitment to reducing the organisation's dependency on consultants.

71. The Security Service also employs two Non-Executive Directors. The Director General explained the value they bring to the Service's work:

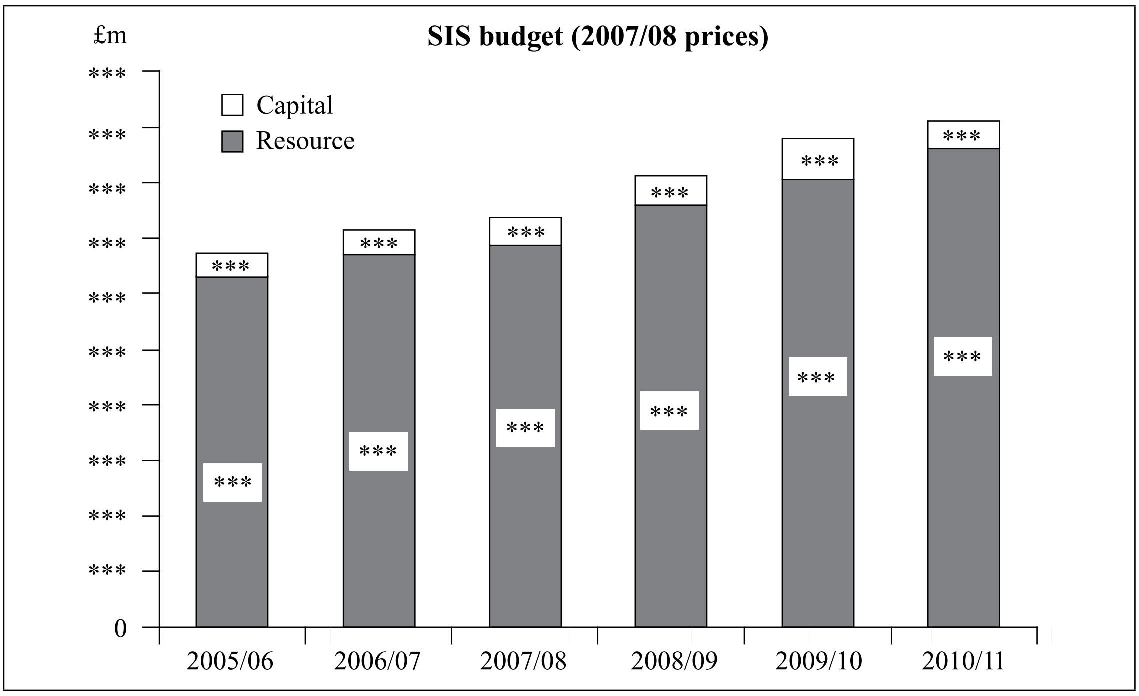
> *It is useful having, at board level… an external view… One of the [Non-Executive Directors] has been hammering away at the need for more clarity on what's going to be delivered when, by whom, what's the deadline and what's the implication if they don't deliver… that clarity in terms of deadlines and clear deliverables has been a big benefit to us… In addition to which, we actually get a great deal of free consultancy out of them and they are very generous in their time and working with… people…*[57]

[57] *Oral evidence – Security Service, 25 March 2008.*

The Secret Intelligence Service

Expenditure

72. The following chart demonstrates the growth in the Secret Intelligence Service's spending.[58]



73. SIS spent £*** million during 2006/07, an increase of 9% over the previous year[59] (compared with the Security Service's 41% increase over the same period).

74. Capital spending for 2006/07 was £*** million, against a budget of £*** million. SIS had planned to spend nearly £*** million to pay for the renovation works taking place at its training facility (***); however, this was delayed until the following financial year (2007/08). These renovations are expected to be completed during 2008, at a total cost of around £*** million.

75. In the CSR07 settlement, SIS was allocated £*** million for 2008/09, increasing to £*** million in 2010/11. It intends to:

- strengthen intelligence collection and covert action overseas;
- develop closer co-operation with UK and overseas partners;
- exploit technology more effectively;

[58] *These figures show spending in 2007/08 prices calculated on the basis of the latest HM Treasury deflators (as at 30 September 2008). As previously indicated (footnote 21), the 2008/09 to 2010/11 figures will be reduced by a £*** million baseline transfer to SOCA.*

[59] *The SIS 2006/07 Resource Account was agreed by the Comptroller and Auditor General in July 2007.*

- manage greater operational risks whilst safeguarding staff and agents; and
- develop and retain high-quality staff from a wider range of backgrounds.

76. The following long-term capital projects will support these priorities:

- "***" (around £*** million over three years) – a programme to enhance connectivity across SIS and its partners in order to give *** access to SIS *** to all *** SIS overseas stations;
- "***" (£*** million across seven years from 2006/07) – a programme of *** to improve connections with overseas stations in harsh environments. It is already deployed in ***, *** and *** and could be deployed elsewhere where needed;
- a proposed £*** million to relocate IT infrastructure in order to free up office space for staff growth; and
- £*** million over seven years on developing and maintaining a document management system to provide email and secure access control to sensitive data.

Policy

International counter-terrorism

77. In 2006/07, over 30% of SIS's effort was directed solely against the counter-terrorism target – although this rises to just under 60% when contributions made by all teams and officers are included. Whilst as a proportion this has remained static since 2005/06, the overall growth in funding means that in real terms it represents an increase in the amount of resources allocated to ICT work.

78. The key priorities for SIS are:

- supporting the growing number of Security Service investigations into terrorist groups and plots;
- continuing its long-term strategic work to penetrate key targets; and
- maintaining and strengthening overseas counter-terrorism liaison capacity.

Work on each of these priorities is detailed in the following paragraphs.

79. The growth in SIS's budget from 2008/09 to 2010/11 will enable it to continue supporting a growing number of Security Service investigations into terrorist activity. This involves both spotting attack planning originating outside the UK and *** terrorist networks overseas. We noted in our 2006–2007 Annual Report the increased proportion of SIS staff working in joint operational teams with the Security Service – 10% of staff in Security Service counter-terrorism casework teams comprise SIS officers (this now includes officers co-located with the Security Service in regional stations across the UK). This closer working enables SIS to improve its support to the Security Service on the overseas aspects of counter-terrorism investigations.

80. Work on long-term strategic targets (including ***) remains a key priority for SIS. This is vital to the UK's requirement to gain intelligence on *** long-term strategies, plans and targets. SIS has established two dedicated teams in London: one looking at developing long-term intelligence-gathering operations and the other focusing on *** and the ***. In support of this work the SIS *** has expanded and is extending its reach beyond ***. As a result of these changes, SIS has been able to illuminate better some aspects of ***.

81. SIS's overseas partnership liaison work involves:

- developing relationships to facilitate information exchange;
- operational exchanges on counter-terrorism work overseas; and
- capacity building (supporting other countries' ability to identify and pursue terrorist suspects themselves, ultimately to prevent terrorist attacks in those countries, and the potential export of terrorists to the UK).

In 2006/07, SIS saw particular improvement in its relationship with a number of key countries (such as ***, *** and ***), and some improvements in others (such as ***). Progress in *** was complicated by the political instability in the country and ***. SIS reported to the Committee that positive relations were maintained with ***.

82. In order to meet its ICT priorities, SIS plans to increase its overseas deployments by more than ***% over the next three years. In order to meet the planned increases in deployments in priority areas, SIS has ended effort in certain areas such as ***, where the *** maintain a significant presence in the region. The UK's intelligence-sharing relationship with these key partners means that SIS no longer needs to maintain a presence in that region (***
***).

Non-ICT work

83. SIS also devotes resources to areas such as ***, *** and the ***; issues such as energy security and regional conflict; and support to military operations.

84. In 2006/07, nearly ***% of its total effort was dedicated to *** – SIS is seeking to increase this in the coming years in order to manage the intelligence requirements arising from ***. The Chief of SIS told the Committee:

> ***
> ***
> ***.[60]

[60] *Oral evidence – Secret Intelligence Service, 24 January 2008.*

85. However, these expansion plans have had to be delayed as a result of ICT work being prioritised. The Chief of SIS told the Committee:

> *A substantial growth in our *** operational capability is definitely part of our service plan. It is happening and it is getting better. I have to say that it is not commensurate with the scale of the issue.*[61]

D. Whilst the Secret Intelligence Service has clearly recognised the wider emerging economic, political and military challenges, we are concerned that diverting resources to tackle the current terrorist threat means that such longer-term challenges might not be receiving adequate attention.

86. SIS devoted just over ***% of its total effort on *** in 2006/07. The Chief of SIS told the Committee that ***
***.

87. In 2006/07, SIS increased its effort in support of UK military deployments overseas. SIS works closely with the ***
***. SIS also undertakes *** reporting for other customers across the same range of targets.

Administration

88. In our 2006–2007 Annual Report, we noted that the National Audit Office (NAO) had identified two cases in SIS's 2005/06 accounts where there had been errors in the reporting of payments to agents. The Committee was assured that steps had been taken to correct the problem. However, the NAO identified a further case in SIS's 2006/07 accounts relating to a £*** loan to an agent for which no repayment schedule was in place. The Chief of SIS told the Committee that this sum represented support *** (linked to an operation) but that, for security purposes, it had been presented as a loan. SIS told the Committee that it has now changed its recording processes to ensure that such expenditure is reflected accurately in its accounts in future.

89. The Committee has previously reported on the internal re-organisation SIS has undertaken (in particular the brigading of teams covering geographic areas into Controllerates). The Committee has been told that this has worked well in bringing together previously separate skills and experience, and in providing a "refreshed" approach to the different challenges of intelligence collection arising in various regions of the world:

> *We are making good progress… [You can] make sure that the best practice that you learn in one area is efficiently and properly applied to operations in another area… [You can also get] the right officers who have got a lot of experience in one area switching quickly to another team and applying the lessons they have learnt in one difficult, hostile environment to another.*[62]

[61] *Oral evidence – Secret Intelligence Service, 11 March 2008.*

[62] *Oral evidence – Secret Intelligence Service, 24 January 2008.*

90. SIS currently has *** permanent staff: this is predicted to increase to *** by March 2009. In 2006/07, SIS recruited *** new staff (slightly above target). A key aim of the recruitment strategy was to achieve a more diverse intake of recruits and SIS therefore used targeted advertising and a combination of local and national media campaigns. Of those recruited, 10% were from black and ethnic minority groups and 34% were female.

91. The growing requirement for SIS staff to operate in potentially volatile and dangerous environments requires very careful risk management on a daily basis. The Chief of SIS told the Committee:

> *The operational environment is more difficult… there is a high security overhead… not just in the actual combat zones… but also in a place like ***… Servicing and keeping ahead of the game in *** stations in *** countries, many of them in combat and difficult zones… there is a big list of issues there.*[63]

The level of risk to the security of staff and their families deployed overseas in high-risk areas is increasing, and SIS has to devote more resource to protecting them. The Agencies' work in these areas is crucial and we commend SIS's efforts to manage the serious risks involved whilst ensuring that vital intelligence collection can be achieved.

92. Last year the Committee recommended that SIS address the issues surrounding its retirement age as a matter of priority. SIS has now implemented the new civil service retirement age of 65 with the exception of senior staff at grade 5 or above, where the retirement age remains ***. The Chief of SIS told us that the issue of senior staff:

> *… is being looked at now very urgently… Our experience tells us… that we need to retain staff beyond ***… we need their experience… Having retirement age as your major mechanism for moving people in and out of senior levels is not a good ideal.*[64]

E. This is the second successive year that the Committee has raised concerns regarding the Secret Intelligence Service's policy on retirement age. We remain concerned that the Service's policy still does not seem fully to meet its business requirements. This should be dealt with as a matter of urgency.

[63] *Oral evidence – Secret Intelligence Service, 11 March 2008.*

[64] *Oral evidence – Secret Intelligence Service, 11 March 2008.*

CROSS-CUTTING ISSUES

Business continuity

93. Following the significant disruption to GCHQ caused by the summer floods in 2007, the Committee undertook to review the business continuity arrangements of all three Agencies.[65]

GCHQ

94. GCHQ has reviewed its business continuity plans following the summer floods of 2007, which resulted in significant disruption to both of its sites ***. The greatest challenge to GCHQ during the crisis was a lack of mains water supply – vital for computer cooling – since both sites held water reserves sufficient for ***. By sending home non-critical staff and switching off a number of non-critical computer systems, GCHQ reduced consumption until suppliers were able to put in place an adequate and reliable supply via road tankers. This allowed critical services to be maintained during the ten-day period during which the mains supply was interrupted.[66]

95. GCHQ identified a number of lessons from these events. We are reassured that, in the main, progress has been made in all the identified areas – reinforced crisis management processes have been put in place and tested, crisis management training has been delivered to key staff, and the vulnerabilities identified during the floods have now been clearly identified and registered. There are some areas, however, that still require progress and we will return to these in the future.

The Security Service

96. In June 2007, the Director General reported that progress had been made in improving the Service's overall business continuity arrangements. The Service has adopted a two-pronged approach to protecting its business:

i. It aims to reduce the risk of disruption with up-to-date protective security measures. The Security Service *** and the Service has, therefore, taken a number of steps over the past year to improve ***. It has also taken business continuity factors into consideration at the early stages of acquiring and developing its new sites across the UK.

ii. It has ensured that, where it has expanded, the new sites add to its overall collective resilience.[67] Loughside, in Northern Ireland, also provides a significant fall-back capability should Thames House suffer significant disruption.

[65] *Cm 7299.*

[66] *GCHQ subsequently ***.*

[67] *Should Thames House be out of action, the Service can now maintain ***.*

97. The Director General has, however, told the Committee that there remain some risks to the resilience of the Service's IT networks. Recent IT improvements have included fall-back facilities at ***, but further developments are planned over the CSR07 period to improve further the resilience of the Service's arrangements, allowing more staff to continue work and sustaining its core business for longer periods.

98. The Director General also told the Committee that he remained concerned that the Service's existing business continuity plan had not been fully tested and so a series of major exercises were planned for 2008.

The Secret Intelligence Service

99. In the Committee's 2006–2007 Annual Report, we noted our concerns about SIS's arrangements for backing up its data and recommended that this was addressed as a matter of priority. We have taken further evidence on the strength of SIS's current arrangements but remain concerned about certain aspects of the arrangements and consider that there is scope for improvement. We note that SIS is currently considering several different options for dealing with this problem, including the use of off-site strategic data centres, and we will therefore review its arrangements next year.

100. SIS's business continuity plan covers a range of scenarios, from the short-term loss of Vauxhall Cross to the complete evacuation of staff out of London for two months. For an incident affecting only part of Vauxhall Cross, SIS would still be able to make use of two separate ***, whilst key staff could be deployed to work out of a number of alternative locations (***). There are also back-up duty officer arrangements for SIS ***.

101. SIS has nearly completed a major programme to duplicate its core IT and communications systems at *** to make it a viable alternative headquarters if Vauxhall Cross were completely out of action as a result of a serious incident. SIS also has a year-round emergency provision in place for the movement of staff out of London, although this does not address a scenario where ***.

102. SIS exercises its evacuation procedures regularly, and plans to hold regular desktop exercises[68] during 2008 to ensure that all teams across the organisation are aware of what to do in an emergency. In view of its dependence upon *** as a back-up site, we would expect SIS to test those arrangements regularly to ensure that they are fully fit for purpose.

103. For staff based overseas, SIS has a critical incident plan covering the Service's response to the death, serious injury or kidnap of an officer or their dependants. SIS is putting in place a Crisis Operations Room specifically to manage any such overseas incidents in future.

[68] *A desktop exercise is designed to simulate an organisation's response to a specific crisis. It tests crisis management and response arrangements and the overall recovery rate (how long it would take to return to normal business).*

Conclusion

F. Following the floods in the summer of 2007, the Agencies have reviewed and improved their business continuity and resilience planning. Whilst we are reassured by the work that has been done so far, and the further changes that are now being made, we consider that there is still scope for improvement.

The Agencies' non-ICT funding

104. The Committee recommended in its 2006–2007 Annual Report that separate additional funding should be made available to safeguard non-ICT work in the face of the increasing focus on counter-terrorism. The Government's response then was that the existing funding arrangements sufficiently take into account the range of national security challenges, and where the Agencies can add greatest value.

105. During the debate on the Committee's 2006–2007 Annual Report in July 2008, the Home Secretary offered the following reassurance:

> *Although the increase in Agency funding was driven largely by the need to respond to the terrorist threat, we continue to resource capabilities to counter other threats effectively. Moreover, capabilities developed to counter terrorism can often be deployed against other targets, and technological advances have led to newer, smarter and more flexible ways of working, which have enhanced our ability to respond to these or any other sudden, unexpected threats.*[69]

G. Whilst the Committee recognises that a single budget ensures maximum flexibility for the Agencies to be able to respond to rapidly changing threats and events, we remain concerned that aspects of the Agencies' work that are not related to international counter-terrorism are continuing to suffer as a result of the focus on counter-terrorism.

Value for money and efficiency in the Agencies

106. HM Treasury savings targets for the Agencies in the CSR07 settlement amount to £***million. In addition to these, the Cabinet Office told us that the Agencies had committed to achieving an extra 3% in efficiency savings during the CSR07 period.

GCHQ

107. GCHQ achieved efficiency savings of £*** million for 2006/07, surpassing its target of £*** million. GCHQ achieved efficiency savings of £*** million for 2007/08, and has agreed efficiency savings with HM Treasury of £*** million for 2008/09, £*** million for 2009/10, and £*** million for 2010/11. It expects to achieve these savings by building on the efficiency achievements made during the SR04 period (2004–07). It will also look to save 5% in its administrative budgets each year, building on its successes over the SR04 period.

[69] *HC Deb 17 July 2008 vol 479 c 456.*

The Security Service

108. In 2006/07, the Security Service reported procurement efficiency savings of approximately £*** million – over 50% higher than the Gershon target.[70] In addition to this, it also achieved a further £*** million of savings in other areas, £*** million of which came from joint working (involving allies sharing a prototype of some communications equipment, which saved the Service around two years worth of research and development). The Director General told the Committee that the Service viewed efficiency savings as *"making money"* – every pound saved can be redeployed towards the Service's key operational priorities. The efficiencies will therefore help the Service to maintain its current capability in the face of inflationary pressures, so that all additional resources provided in the CSR07 settlement can be used to provide additional front-line capability. The Security Service achieved efficiency savings of £*** million for 2007/08 and has forecast efficiency savings of £*** million for 2008/09, £*** million for 2009/10 and £*** million for 2010/11.

The Secret Intelligence Service

109. SIS achieved efficiencies of nearly £*** million for 2006/07, £*** million more than its target. A significant proportion of these savings was achieved by renegotiation of SIS's *** and an additional £*** million was saved by switching *** to a different supplier.[71] As part of the Comprehensive Spending Review, SIS carried out a review of expenditure in a number of areas. As a result, it has produced plans setting out how maximum value for money will be delivered from procurement, facilities management, HR and work on serious crime. SIS achieved its planned efficiency savings of £*** million for 2007/08 and has forecast efficiency savings of £*** million for 2008/09, £*** million for 2009/10, and £*** million for 2010/11.

Monitoring performance

110. The Committee has been told that, in view of the substantial budget increases allocated to each of the Agencies, the Cabinet Office and HM Treasury were working with the Agencies to develop a framework for monitoring efficiency and effectiveness. As a result, from autumn 2008, HM Treasury will conduct six-monthly stocktakes of the Agencies' performance, including examining progress on delivery of departmental strategic objectives, value for money, efficiencies and financial management of the Single Intelligence Account.

H. The Committee welcomes the work being done to establish a new framework for monitoring the performance, efficiency and financial management of the Agencies. The Committee is also considering, in consultation with the Agencies, ways in which its oversight of the Agencies' budgets can be conducted in a more timely way.

[70] *In 2004 Sir Peter Gershon conducted a review of public sector efficiency. He made a series of recommendations for how departments could achieve year-on-year efficiency savings. Since 2004, the Agencies have agreed annual "Gershon" efficiency savings with HM Treasury.*

[71] *The *** is an annual sum *** to cover the cost of ***.*

Media relations

111. In our last Annual Report we reported the concerns that had been raised with us about media relations and recommended that the Government engage with the media to improve the systems for handling national security information. The Committee acknowledges the important work carried out by the media and the Government to protect sensitive information relating to national security and notes that the Defence, Press and Broadcasting Advisory Committee (DPBAC) regularly reviews the content of Defence Advisory (DA) Notices in order to take account of the current terrorism threat.

112. Nevertheless, details of sensitive counter-terrorism operations have been made public before it was safe to do so – as shown by the press leaks during Operation GAMBLE in 2007 – and this has been, rightly, raised with us as being of concern. We will therefore look to discuss with all those concerned whether the current system provides adequate protection whilst maintaining the ability of the media to report on matters of public interest.

STRATEGIC FRAMEWORK AND INTELLIGENCE MACHINERY

113. The Committee reported in its 2006–2007 Annual Report on the outcome of the Home Secretary's review of the Government's counter-terrorism policies, approach and structures. The review had recommended two key changes – the establishment of the Office for Security and Counter-Terrorism (OSCT) in the Home Office, and a new Ministerial Committee on National Security, International Relations and Development (NSID).

The Office for Security and Counter-Terrorism and CONTEST

114. The OSCT was established in March 2007 to take over co-ordination of the Government's counter-terrorism strategy, CONTEST, and some aspects of its delivery. As at February 2008, it comprised 270 permanent staff based in the Home Office. The OSCT is designed to:

> *… bring a new drive, more cohesion and greater strategic capacity to our fight against terrorism… and deliver a system that is inclusive and integrated, with added capacity and political oversight.*[72]

115. As part of this work it was tasked with a "refresh" of CONTEST. The Home Office told us:

> *We are taking CONTEST apart and putting it back together again… We have looked quite extensively at the delivery of CONTEST…*[73]

A number of departments and the Agencies have been involved in the refresh of CONTEST, which the Home Office said would be finished by autumn 2008 – the Committee is awaiting an update on the outcome of this work.[74] The changes implemented thus far have included the development of detailed delivery plans for each strand of CONTEST, the introduction of a new counter-terrorism public service agreement (PSA) and the development of a new capability[75] to detect emerging future threats.

116. One of the key changes that has already resulted from the review is a renewed focus on the PREVENT strand of the strategy. The Home Secretary told the Committee:

> *… The fact that we have been able, working across government, to bring together the framework for delivering the PREVENT work… able to agree for the first time across government what the strategic objectives of that should be, is precisely the type of co-ordination of both strategy and delivery that was envisaged when we set up the Office.*[76]

[72] *Letter from the Home Office, 1 April 2008.*

[73] *Oral evidence – Home Office, 5 February 2008.*

[74] *As at 7 November 2008.*

[75] *This horizon-scanning capability forms an important element of future planning for CONTEST, allowing better anticipation of future threats.*

[76] *Oral evidence – Home Secretary, 5 February 2008.*

117. The PREVENT strategy's aim is to *"stop people becoming terrorists or supporting violent extremism"*. It seeks to achieve this by:

- challenging the ideology behind extremism and supporting mainstream voices;
- disrupting those who promote violent extremism and those who support the institutions where they operate;
- supporting individuals who are vulnerable to recruitment by proponents of violent extremism;
- increasing the resilience of communities against violent extremism; and
- addressing the grievances that ideologues are exploiting.

The OSCT has begun to put in place some practical measures to achieve these aims, including:

- providing funding for 200 community projects aimed at preventing violent extremism;
- a police PREVENT strategy and delivery plan, with 300 new PREVENT officers planned;
- working to improve take-up of citizenship education programmes in mosque schools;
- providing funding to youth offender panels for programmes to support individuals vulnerable to extremist ideology;
- a major programme to tackle radicalisation in prisons; and
- a new strategic communications unit in order to counter the impact of terrorist propaganda and promote a revised approach to the use of official language and tone.

118. In order to counter terrorist messages, the Research, Information and Communications Unit (RICU) was set up at the same time that the OSCT was formed. RICU advises departments across government on communicating counter-terrorism and counter-extremism messages and works to ensure that those messages are consistent. It provides a unified strategy across all departments involved in delivering aspects of PREVENT.

119. The Home Office told us during our Review of the Intelligence on the London Terrorist Attacks on 7 July 2005 that it is still too early to measure real success or outcomes of the new strategy. Therefore, whilst it appears that this work is now on a sounder footing, we will monitor progress.

Ministerial Committee on National Security, International Relations and Development

120. The Ministerial Committee on National Security, International Relations and Development (NSID) is chaired by the Prime Minister and its terms of reference are *"to consider issues relating to national security, and the Government's international, European and international development policies"*. It has met three times in total since it was established in July 2007, and its sub-committees (which are chaired by the Prime Minister or senior Cabinet colleagues) have met 30 times. A range of topics has been considered during this time, including "Afghanistan Strategy", "Zimbabwe", "Security Screening of Health Employees" and "Security of the 2012 Olympics".

121. We reported last year that we were pleased that a new Committee had been established to enable Ministers to meet formally to discuss intelligence and security issues, in the absence of any regular meetings of the Ministerial Committee on the Security and Intelligence Services (CSI). This already appears to be showing benefits – the Cabinet Secretary told us: *"as you can see from the number and frequency of the meetings, it is actually happening. This is much more real."*[77]

The National Security Strategy

122. One of NSID's first recommendations, in July 2007, was to publish a National Security Strategy. The strategy – eventually published in March 2008 – lists the key threats and risks facing the UK as being:

- terrorism;
- nuclear weapons and other weapons of mass destruction;
- trans-national organised crime;
- global instability (including conflict and failed and fragile states);
- civil emergencies; and
- state-led threats to the United Kingdom.

It sets out how the Government will:

> *… address and manage this diverse though interconnected set of security challenges and underlying drivers, both immediately and in the longer term, to safeguard the nation.*[78]

[77] *Oral evidence – Cabinet Secretary, 29 April 2008.*

[78] *Cm 7291.*

123. We have questioned whether the strategy will achieve any benefits in real terms or whether it is simply a paper exercise. The Foreign Secretary told the Committee:

> *I see a number of benefits. First, it does join up the different aspects of national security or the way in which we are tackling national insecurity… Secondly, I think that it helps us check that we have the right degree of focus and drive in the key areas. Thirdly… part of the purpose… is to take the discussion out into the country so that there is a wider… understanding of some of the threats that we face… I think in those ways that the security strategy can help, but it would be wrong to say it would be a massive change. It's drawn together some existing work… in that sense it is useful.*[79]

124. The National Security Strategy does not create new areas of responsibility for the Agencies or the wider intelligence community. The Heads of the Agencies have indicated that they were consulted about the strategy and are broadly supportive of it, but that they do not envisage that it will result in any significant change in direction for them. The Cabinet Secretary told us that it does require the Agencies and departments to be *"much clearer about the way in which they are working together and the way in which their strategies actually fit",*[80] and the Head of Intelligence, Security and Resilience told us that the National Security Strategy will have a direct bearing on the way in which the requirements and priorities for the intelligence community are set in the future.[81]

125. At the same time as the Prime Minister announced the National Security Strategy, he also outlined plans for a National Security Forum, consisting of business, academics, community groups, and military and security experts. The aim of the new forum is to:

> *… harness a much wider range of expertise and experience from outside government, and to help us plan for the future… [The forum will] advise the … National Security Committee.*[82]

126. In July 2008, the Prime Minister announced that the National Security Forum would comprise a core group of 12 members with expertise covering the range of threats and risks outlined in the National Security Strategy. Its role will be to provide advice to NSID, and it will also be able to commission research on national security-related matters. The forum will be supplemented by a register of experts who could be called upon to provide specific advice and expertise as required. There will also be a dedicated Cabinet Office Secretariat to support the work of the National Security Forum. How the role of the National Security Forum will develop, and what value it will add, remain to be seen.

[79] *Oral evidence – Foreign Secretary, 8 April 2008.*

[80] *Oral evidence – Cabinet Secretary, 29 April 2008.*

[81] *The Joint Intelligence Committee requirements and priorities are discussed in detail in paragraph 140.*

[82] *HC Deb 19 March 2008 v 473 c 926. We understand that the National Security Committee is what is now referred to as NSID.*

127. In the same statement, in July 2008, the Prime Minister also outlined proposals for oversight of the National Security Strategy:

> *I propose… to consult [on]… the establishment and terms of reference of a joint committee on the National Security Strategy comprising the Chairs of the key Departmental Select Committees with an interest in national security and other Members of Parliament and Peers with particular interests or experience.*[83]

128. The Committee will continue to oversee those aspects of the National Security Strategy that impact on the work of the intelligence and security Agencies, and on others involved in secret intelligence work.

The Head of Intelligence, Security and Resilience

129. In our last Annual Report we commented on changes to the role of what was previously known as Permanent Secretary, Intelligence, Security and Resilience.[84] This role was initially created in September 2005, amalgamating the two previously separate roles of Joint Intelligence Committee (JIC) Chairman and security adviser to the Prime Minister. The Cabinet Secretary told the Committee at the time that the rationale for merging these two roles was to add weight and authority to the JIC Chairman role, establishing the JIC Chairman as senior amongst JIC colleagues, including the Agency Heads.[85]

130. In July 2007, however, the Prime Minister announced to Parliament that, in line with the recommendation in the Butler Review, the role would again be split into its two previous components – the Chairman of the Joint Intelligence Committee[86] and the adviser to the Government on intelligence and security matters (now called the Head of Intelligence, Security and Resilience).[87] Responsibility for the Single Intelligence Account (SIA) and for the performance management of the Agency Heads would pass to the Cabinet Secretary.

131. Whilst we welcomed the separation of the two roles, we were disappointed that the grade of both posts was now lower than it had been when they were combined and that effectively the position has reverted to its pre-2005 grade – which leaves the original problem regarding the seniority of the JIC Chairman role, and creates a similar problem in respect of the security adviser to the Prime Minister. We wrote in our 2006–2007 Annual Report that we were *"concerned at the impact this may have on relationships between the holders of these posts and the Heads of Agencies, who are of a higher grade"*.[88]

132. We returned to these changes again this year. We questioned the new Head of Intelligence, Security and Resilience on how the new structure was working, in particular his relationship with the Heads of the Agencies. He told us:

[83] *HC Deb 22 July 2008 vol 479 c 112ws.*

[84] *Cm 7299, paragraph 73.*

[85] *Cm 6864, paragraph 8.*

[86] *Alex Allan came into this post in January 2008.*

[87] *Robert Hannigan came into this post in September 2007 and took over full responsibility following Sir Richard Mottram's retirement in November 2007.*

[88] *Cm 7299, paragraph 76.*

> *I see them all individually and collectively very regularly. In some senses… it has been the best of both worlds in that they know that [the Cabinet Secretary] is the person they see for their annual appraisal and that they see regularly on intelligence matters… and on specific issues… but they accept that he is not going to do the day-to-day handling particularly of the SIA. So it seems to work pretty well… It is all about relationships. If they trust you, they will be much more open with you…*[89]

133. The Cabinet Secretary told us that his new role overseeing the performance of the Heads of the Agencies *"does give me a more active engagement with them about their objectives and how they are performing against their objectives"* and that taking on the responsibility of Accounting Officer for the SIA was consistent with that role.[90] He therefore thought that the new arrangements were working well but that he *"still had a slightly open mind"* about the structures and would therefore continue to monitor how well they were working.[91]

I. The Committee welcomes the separation of the roles of Chairman of the Joint Intelligence Committee and the security adviser to the Prime Minister. We remain convinced, however, that for them to function effectively both posts must be at an appropriately senior grade.

J. Whilst the Committee welcomes the Cabinet Secretary's increased involvement in intelligence matters at a strategic level, we question the amount of time he can, in reality, give to his new line management role with the Agency Heads, in view of his other responsibilities. We will keep this arrangement under review.

The Professional Head of Intelligence Analysis

134. The Butler Review identified the need for a career specialism in intelligence analysis which incorporated development, training and career advancement. As a result, the role of the Professional Head of Intelligence Analysis (PHIA) was created to provide a "champion" for analysts, and to establish a distinct career specialism for this group. The Committee reported in its 2006–2007 Annual Report that the PHIA was fulfilling an important role in ensuring effective intelligence analysis training and closer working between analysts across the intelligence community.

135. We are therefore very concerned that the post remained vacant since Jane Knight (the first post-holder) retired in August 2007. We are particularly concerned that the progress achieved during the previous two years may be lost. Although we note that the Deputy Professional Head has been covering both posts during this time, we question the extent to which one person can adequately cover two demanding posts at the same time. The JIC Chairman told us in January 2008 that thought was being given to the future of the Professional Head post – whether it should be a separate post, or whether it should be amalgamated within the JIC Chairman role. The Cabinet Office has since told us that a decision has been made to subsume the role within the JIC Chairman role.

[89] *Oral evidence – Head of Intelligence, Security and Resilience, 29 April 2008.*

[90] *Oral evidence – Cabinet Secretary, 29 April 2008.*

[91] *Oral evidence – Cabinet Secretary, 29 April 2008.*

K. Given the importance of the Professional Head of Intelligence Analysis (PHIA) post, we are very concerned by the plan to subsume the role within the Joint Intelligence Committee Chairman's post as this may actually lessen the priority given to this crucial role. The Committee is disappointed that the PHIA post has not been maintained as a distinct and separate role.

The Joint Terrorism Analysis Centre

136. The Joint Terrorism Analysis Centre (JTAC) is a multi-agency organisation that analyses and assesses the threat from international terrorism, and uses these assessments to set the UK threat level. This contrasts with the JIC and Assessments Staff in the Cabinet Office, which generate more strategic product focusing on a wide range of topics over and above international terrorism.

137. As a result of the "refresh" of CONTEST, and PREVENT in particular, the Government identified a need to understand better what led individuals from different communities, including universities, prisons and cyberspace, to develop extremist views and support or engage in violent extremism. As a result of this, in March 2008 the Prime Minister announced a 10% increase in resources for JTAC for a new team with *"a new focus on the longer-term challenge of investigating the path to violent extremism"*.[92] Whilst JTAC's traditional focus is on current and immediate threats based on secret intelligence, the new team will use a range of sources other than secret intelligence.[93] The Director General of the Security Service explained:

> *So the intention is that there will be, within JTAC… a small number of people who will be drawing probably not on secret intelligence… in order to provide a context within which government can decide how best to try and intervene to stop people drifting towards the radical edge of the faith and then potentially out into terrorism.*[94]

L. The Committee agrees that there is a need to improve understanding of "the path to extremism" and welcomes the establishment of a new team analysing open-source and academic material in this field. However, the team does not appear to sit comfortably within the Joint Terrorism Analysis Centre (JTAC). One of the key strengths of JTAC is its operational focus on the immediate threat from international terrorism – this should not be diluted in any way. Consideration should therefore be given to moving this new team to a more appropriate location (such as the Office for Security and Counter-Terrorism in the Home Office), with the establishment of a clear liaison function as necessary.

[92] *HC Deb 19 March 2008 vol 473 c 926.*

[93] *The new team will use open-source material, academic research and survey data in addition to secret intelligence and will take on some of the PREVENT work previously undertaken by other parts of JTAC.*

[94] *Oral evidence – Security Service, 25 March 2008.*

The Centre for the Protection of National Infrastructure

138. The Centre for the Protection of National Infrastructure (CPNI) is an inter-departmental centre which was formed in February 2007 by amalgamating two previous organisations: the National Security Advice Centre (NSAC), a part of the Security Service that provided advice on physical and personnel security matters, and the National Infrastructure Security Co-ordination Centre (NISCC), an interdepartmental centre that provided advice on Information Assurance matters. The Security Service is a major contributor to CPNI[95] and the Director General of the Security Service told us that the amalgamation has provided customers with a single point of contact for protective security advice. The restructuring work has enabled CPNI to focus on providing integrated advice on national security threats, including to sectors of the economy that are not part of the Critical National Infrastructure (CNI),[96] such as companies in the chemicals, aerospace and pharmaceuticals sectors.

The Joint Intelligence Committee and Assessments Staff

139. The Joint Intelligence Committee (JIC) in the Cabinet Office is responsible for providing co-ordinated intelligence assessments on a range of national security and defence matters.

140. The JIC is also responsible for approving the UK's requirements and priorities (R&Ps) for secret intelligence collection and assessment, prior to endorsement by the Ministerial Committee on the Security and Intelligence Services (CSI).[97] The R&Ps are determined by the Government's strategic priorities for defence and security, foreign policy, economic wellbeing, and the prevention or detection of serious crime. Last year's R&Ps gave top priority to seven areas:

- ***;
- ***;
- ***;
- ***;
- ***;
- ***; and
- ***.

141. The Assessments Staff, consisting of analysts drawn from a range of departments and agencies, supports the work of the JIC. During 2007/08, the Assessments Staff produced over 200 intelligence assessments – the largest number produced in the last four years. The Chief of the Assessments Staff told us that the increase in output was largely due to the number of rolling assessments produced for COBR:[98]

[95] ***.

[96] *The UK's national infrastructure is those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of essential services. It is made up of nine sectors: energy, food, water, transport, communications, government, emergency services, health and finance. Those parts of the sectors which, if lost or compromised, would have a highly detrimental impact on the availability of essential services are known as the Critical National Infrastructure.*

[97] *The R&Ps are reviewed annually and cover a three-year period.*

[98] *COBR is the Cabinet Office Briefing Room, which is used during a crisis. Rolling assessments are produced for COBR and updated as intelligence comes in, sometimes more than once a day.*

> *Our output has been increased really because of a whole series of running crises there [in COBR]. We had the Alan Johnston kidnap. We had the British diplomats who were taken hostage in Ethiopia/Eritrea, in the spring. We had, of course, the attacks in London and Glasgow, where COBR ran for a considerable period of time. Then, more recently, we have had *** the Baghdad hostages as well. I think it is worth mentioning that, because it is a demand on the Assessments Staff, because we do manage and produce these rolling assessments for COBR meetings, although it does not feature, if you like, in the statistics that come to you routinely.*[99]

142. In terms of subject matter, Iraq remained a key focus but there was also an increased focus on Afghanistan as a result of troop deployment there and the Assessments Staff have therefore redeployed an analyst to reinforce work on South Asia. The JIC has also increased its work on energy security during 2007/08 and considered issues such as the implications of climate change for global security and stability, and the implications of ***.

143. The new JIC Chairman told the Committee that one of his priorities coming in to the post was:

> *To make sure that what we do in the JIC is focused on the particular priorities and unfolding events, but that we do keep an eye on what is the big picture. Are we deploying our resources effectively, and avoiding the sort of "it will be very interesting to look at" something that might be interesting but is low priority… We need to make sure that we use the JIC as a top-level committee, to make sure that we are thinking strategically about what are the key issues.*[100]

144. One of the changes made previously that seems to be working well is the Challenge Team, established two years ago as a result of the Butler Review,[101] which identified the need for a "challenge function" to be built into the intelligence analysis process. The Chief of the Assessments Staff told us:

> *When we set the team up… there were a number of discrete projects I wanted to undertake looking at particular areas of JIC work, going back some way… These were areas where in some cases customers had questioned whether we had a particular mindset and were unwilling to challenge ourselves enough. In some cases I had wondered whether our judgements were as robust as they could be…*[102]

145. Examples of subjects the Challenge Team have looked at include assessments on ***
***.

146. Whilst these reviews are highly important, the second part of the Challenge Team's role – to ensure that the concept of challenge is embedded throughout the Assessments Staff – is perhaps even more important. The Chief of the Assessments Staff told us:

[99] *Oral evidence – Cabinet Office, 8 January 2008.*

[100] *Oral evidence – JIC Chairman, 8 January 2008.*

[101] *HC 898.*

[102] *Oral evidence – Cabinet Office, 8 January 2008.*

> *In a way, one of the Assessments Staff's functions in leading [discussions] on any subject is to draw on, take the experts' views and subject them to tests, to challenge, whether it is the collectors to challenge their confidence in their sources or whether it is the experts in, say, the Defence Intelligence Staff or the Foreign Office in their areas of expertise, just to put the contrary view and to test it.*[103]

M. The Committee considers that the challenge process is vital to ensuring that the Joint Intelligence Committee product is of a good quality and must be encouraged.

SCOPE

147. SCOPE is a major cross-government IT programme aiming to improve the intelligence community's secure communications. The Committee has repeatedly raised concerns about delays to this project, a lack of preparation amongst partner departments, and the risks to the successful delivery of Phase II:

> *We remain very concerned, however, by the numerous delays… a general lack of preparedness for full implementation amongst SCOPE partners, and difficulties in providing a secure environment for the deployment of SCOPE overseas.*[104]

148. Last year we reported that Phase I had finally been implemented, but expressed concern at further delays to Phase II – which aimed to broaden the user departments and improve capability of their communications. This phase had been delayed and revised on a number of occasions. Last year we were told that considerable work had been done to reduce the risk of any further delay and to ensure its successful delivery between mid-2008 and early 2009.

149. This year, however, the Cabinet Secretary told us that, despite all this work, Phase II of SCOPE has now been abandoned:

> *… we know that the way they were planning to do [Phase II] won't work… So we are working actively on ways in which we can achieve those benefits, but probably through rather different routes.*[105]

150. At the time of writing, the Committee has yet to be provided with details of how the decision to scrap SCOPE Phase II was arrived at, what the cost implications are and what the options are for a replacement system.

N. We have consistently reported concerns about SCOPE and are appalled that Phase II of the system – on which tens of millions of pounds have been spent – has now had to be scrapped. We sincerely hope that lessons have been learnt from this failure and that they will be used when plans for the future are being drawn up. We also expect the development of any replacement capability to be subject to more stringent controls, and greater management and financial accountability, from the outset. We will be investigating the reasons for the serious failure of this important project, and will report on the matter in the forthcoming year.

[103] *Oral evidence – Cabinet Office, 8 January 2008.*

[104] *Cm 7299, paragraph 90.*

[105] *Oral evidence – Cabinet Secretary, 29 April 2008.*

The Defence Intelligence Staff

151. The Defence Intelligence Staff (DIS) in the Ministry of Defence (MoD) remains the largest all-source analytical capability in the intelligence community, employing nearly 450 analysts in this role. Much of its output is in direct support of UK military operations in Iraq and Afghanistan and, to a lesser degree, UK deployments in the Balkans.

152. During 2006/07, DIS has:

- maintained its unique capability to generate products from all-source analysis to support operational decisions;
- continued to produce in-depth analysis contributing both to force deployment decisions and strategic foreign policy decisions;
- provided a global horizon-scanning capability which gives advanced warning of where UK military resources might be called upon for assistance; and
- doubled the number of teams within the Defence HUMINT Unit that are able to operate in military theatres.

153. On counter-terrorism, DIS contributes to the wider UK intelligence community, providing military technical expertise on the types of threats that might be faced by the UK. In addition, around 20 DIS staff are based within the Joint Terrorism Analysis Centre, providing a range of analytic and other support.

Modernisation

154. DIS has continued to implement its modernisation strategy in order to ensure that it has the capability to meet key customers' long-term requirements. The Intelligence Collection Group (ICG) was established in 2006 to integrate DIS's specialist intelligence collection capabilities both in the UK and overseas. The Committee has been told that the benefits of this include greater co-operation and integration between the various intelligence disciplines within the ICG, and indeed across the wider UK intelligence community. Around half of the ICG's output during 2006 was in direct support of UK military operations – this included a range of new integrated intelligence products routinely combining mapping, imagery and signals intelligence (SIGINT). The Chief of Defence Intelligence told the Committee:

> *We're able to bring the capabilities together when we are back in the UK so that they feed off each other and we can have a more dynamic relationship between [them].*[106]

155. We reported last year on plans to move JARIC[107] from its current location at RAF Brampton to a new facility at RAF Wyton, where it will be co-located with ICG headquarters – we understand that there are plans for the move to take place at some stage between 2009 and 2011. The Chief of Defence Intelligence told the Committee that there were also plans in place to move all the operational elements of the HUMINT organisation into the ICG, thus uniting all aspects of military HUMINT. We understand that this move has now taken place.

[106] *Oral evidence – Chief of Defence Intelligence, 26 February 2008.*

[107] *JARIC (the Joint Air Reconnaissance Intelligence Centre) is also known as the National Imagery Exploitation Centre.*

Staffing

156. The Secretary of State for Defence announced plans in October 2007 to reduce staffing numbers across the Ministry of Defence, including a 25% reduction in staff working out of the MoD headquarters in London, where DIS is based. The Chief of Defence Intelligence told the Committee that, in relation to these plans:

> *My main effort with my colleagues… is to make sure that we respect and protect those elements of our capability which are for the nation and do not do anything to damage either our capability or indeed our reputation.*[108]

157. In August 2008, the Committee was told that, as part of the MoD's streamlining plans, the DIS:

> *… will be reorganised to make it more agile and customer focused while delivering process and efficiency savings of about 20%… This will mean a reduction in some support provided to external partners.*[109]

In response to further questions from the Committee, we have now been told that the streamlining means a reduction of 20% of posts based in Whitehall.[110]

O. The Defence Intelligence Staff (DIS) is a critical part of the UK intelligence community, and the single largest intelligence analytical capability in the UK. Its analysts are highly trained intelligence officers with a broad range of experience and knowledge who collectively make a critical contribution to the overall UK intelligence effort. Whilst the Committee understands that only 16% of DIS staff are based in Whitehall, it is, nevertheless, where its analysts are based, and therefore a cut in the number of Whitehall staff must mean a reduction in DIS's analytical capability. The Committee is therefore concerned by the possible impact on DIS's analytical capability of these efficiency savings and staff cuts, particularly when viewed against the very significant increases in resources that the Security Service, Secret Intelligence Service and GCHQ have received.

The Commissioners

158. The work undertaken by the Intelligence Services Commissioner and the Interception of Communications Commissioner is critical to maintaining public trust that the Agencies operate within the law in relation to their use of intercepted communications and surveillance.[111] The Committee held informal discussions with the Commissioners this year given its common interest in areas such as the use of intercept as evidence in criminal trials, the Wilson Doctrine[112] and intelligence oversight.

[108] *Oral evidence – Chief of Defence Intelligence, 26 February 2008.*

[109] *Letter from the Ministry of Defence, 22 August 2008.*

[110] *Letter from the Ministry of Defence, 1 October 2008.*

[111] *The Regulation of Investigatory Powers Act 2000 is the legal framework which regulates the Agencies' activities in this area.*

[112] *The Committee looked at this in its 2005–2006 Annual Report (Cm 6864, p11).*

159. The Intelligence Services Commissioner, Sir Peter Gibson, reported that there continued to be intensive counter-terrorism-related surveillance activity during 2007, at similar levels and patterns to the nine months covered in the previous year's report. The number of reported errors during 2007 was slightly less than that reported for the previous year.[113]

160. The Interception of Communications Commissioner, Sir Paul Kennedy, reported that there was only a slight increase in the number of warrants issued by the Home Secretary during 2007 compared with the previous year. There were no significant changes in the patterns of requests for warrants. In respect of errors, again, the number reported for the whole of 2007 was similar to that reported for the nine months covered in the 2006 annual report – all the reported errors were genuine procedural or technical mistakes and were reported without delay.[114]

161. Both Commissioners have said that they have been impressed by the Agencies' approach and professionalism.

Official Secrets Act

162. We previously reported on the need for the Official Secrets Act to be amended and our concern that time could not be found in the legislative programme to do this.

163. The Home Secretary[115] told us this year that recent case law has meant that the need for reform is now less urgent. The Home Office explained:

> *In the Shayler case,[116] the Court of Appeal indicated that the common law defence of duress of circumstances would be available in theory against a charge under the Act. Since then, cases where the defence has been raised have clarified that duress would need to be direct and imminent for the defence to succeed. There would need to be a real and immediate threat to the defendant or someone for whom he is directly responsible.*
>
> *The House of Lords considered the defence of duress in R. v Hasan 2005 UKHL 22. Lord Bingham stated that "where policy choices are to be made, [he was inclined] towards tightening rather than relaxing the conditions to be met before duress may be successfully relied on." In the light of that clarification, the need to revise the Official Secrets Act in this respect is no longer as pressing.[117]*

[113] *The Report of the Intelligence Services Commissioner for 2007 was published on 22 July 2008 (HC 948).*

[114] *The Report of the Interception of Communications Commissioner for 2007 was published on 22 July 2008 (HC 947).*

[115] *The Official Secrets Acts 1911–1989 are now the departmental responsibility of the Ministry of Justice.*

[116] *David Shayler was convicted under the Official Secrets Act in 2002 of passing to a newspaper information and documents obtained by virtue of his employment in the Security Service.*

[117] *Letter from the Home Office, 1 April 2008 (underline added).*

OTHER ISSUES

Rendition report

164. In July 2007 the Committee published its inquiry into rendition. Since that report was published there have been a number of developments related to rendition flights through Diego Garcia and a number of allegations of UK Agencies' complicity in the alleged mistreatment of individuals detained overseas. The Committee is therefore now revisiting some of the matters in its original report.

165. Due to the possibility of future legal proceedings in relation to some of these matters and the need to conclude inquiries on other matters, the Committee is unable to comment further at this stage. We intend, however, to report in full when we are able to do so.

Intercept as evidence

166. In July 2007, the Prime Minister established a cross-party Privy Council Review, led by the Rt. Hon. Sir John Chilcot (the Rt. Hon. Sir Alan Beith MP was a member of the Review), to:

> *… advise on whether a regime to allow the use of intercepted material in court can be devised that facilitates bringing cases to trial while meeting the overriding imperative to safeguard national security.*[118]

167. This Committee took evidence from the Agencies on the impact that using intercept as evidence would have on their work and reported our findings to the Chilcot team. We concluded that:

> *Any move to permit the use of intercept evidence in court proceedings must be on a basis that does not jeopardise that capability.*[119]

168. The Chilcot Review was published in February 2008 and concluded that:

> *… we agree with the principle that intercept as evidence should be introduced… However, the ability to prosecute serious organised crime and terrorism is only one way of achieving the protection of the public. We would therefore support intercept only if, on balance, it would at one and the same time safeguard national security, facilitate bringing cases to trial and allow the effective use of intercept as intelligence to continue.*[120]

[118] *Cm 7324.*

[119] *Cm 7299.*

[120] *Cm 7324.*

169. The Review therefore recommended a set of nine requirements that would need to be satisfied before intercept could be used as evidence:

i. The intercepting agency shall decide whether a prosecution involving its intercepted material shall proceed.

ii. Intercepted material originating from the intelligence agencies shall not be disclosed beyond cleared judges, prosecutors or special advocates, except in a form agreed by the originating agency.

iii. Material intercepted using sensitive SIGINT techniques shall not be disclosed unless the Secretary of State is satisfied that disclosure would not put the capability and techniques at risk.

iv. No intelligence… agency shall be required to retain raw intercepted material for significantly more or less time than needed for operational purposes.

v. No intelligence… agency shall be required to examine, transcribe or make notes of intercepted material to a substantially higher standard than it believes is required to meet its objectives.

vi. Intelligence… agencies shall be able to carry out real-time tactical interception in order to disrupt, interdict or prevent terrorist and criminal activity, as effectively as they do now.

vii. Law enforcement agencies shall be able to use interception to provide strategic intelligence on criminal enterprises, and retain the intelligence sometimes for a number of years, regardless of the progress of specific criminal cases. Interception from the same lines may serve both tactical and strategic purposes; if it does, it shall be handled in a manner appropriate to both.

viii. Intelligence agencies must be able to support law enforcement by carrying out interception for "serious crime" purposes of targets nominated by law enforcement, and to provide the product of reports on them to those agencies. Anything so provided shall be subject to the same disclosure obligations as other intelligence intercept.

ix. At trial (whether or not intercept is adduced as evidence) the defence shall not be able to conduct successful "fishing expeditions" against intercept alleged to be held by any agency.

170. The Government accepted the Review's recommendation and set up an Implementation Team based in the Home Office, working closely with those organisations that use and retain intercept material. The Implementation Team reports to a Steering Group comprising senior representatives from within the interception community. Additionally, an Advisory Group of Privy Counsellors[121] has been established to advise the Implementation Team. The Committee has been told that there are three key phases:[122]

[121] *This comprises the original members of the cross-party Privy Council Review with the exception of the Rt. Hon. Lord Hurd of Westwell, who has been replaced by the Rt. Hon. Michael Howard MP.*

[122] *Letter from the Home Office, 29 May 2008.*

- identifying and addressing the key structural issues involved (expected to be completed by the end of October 2008);
- preparing draft legislation and drawing up operational guidance (expected to be completed by the end of February 2009); and
- testing the framework that has been developed to ensure that the Chilcot tests will be met in practice (expected to be completed by the end of June 2009).

We have also been told that, subject to the Chilcot requirements being met, legislation to allow intercept material to be admissible in criminal trials could be introduced in 2009 or 2010.

171. The Director of GCHQ told us:

> *It will be very difficult because that set of tests articulates very clearly the set of concerns we have been voicing over the years as the reasons why doing it wrong would give us a very, very serious blow back to our capability. If it were easy, or even only mildly difficult, I think we would have found the answer by now. So this is not going to be something where people say in two or three weeks' time, "That was easy. We've done that." This is a very difficult job.*[123]

P. We welcome the fact that the Chilcot conditions meet our concerns that the Agencies' capability must not be damaged should their intercept material be adduced in court. We are concerned, however, as to whether it will be possible to meet these conditions.

172. We also note that the Counter-Terrorism Bill 2008 included a provision for the use of intercept material to be disclosed in certain circumstances in inquests and also to allow disclosure to Counsel to an inquiry[124] that falls under the Inquiries Act 2005. The Committee asked the Home Office for clarification as to whether the Chilcot conditions would be met in these circumstances. The Home Office told us:

> *The reality is that this is a difficult issue that we have to resolve irrespective of the outcome of that work… There will only be a very limited number of circumstances in which we envisage the coroners' measures being used.*[125]

173. Whilst we note the safeguards in the Regulation of Investigatory Powers Act 2000 prohibiting disclosure of intercept beyond the "circle of secrecy", we remain concerned by the possibility of intercept disclosure in the event of a judicial review arising out of coroners' proceedings in which intercept material was used. We were therefore pleased that this provision was removed from the Counter-Terrorism Bill in October 2008. We note that the Home Office has said that it may be included in future legislation – if this is the case, the concerns we have raised will need to be considered at that stage.

[123] *Oral evidence – Director of GCHQ, 19 February 2008.*

[124] *The panel of such an inquiry can already request intercepted material to be disclosed to them.*

[125] *Letter from the Home Office, 9 July 2008.*

Interception modernisation

174. The ability to intercept communications is essential to the UK's national security. This ability is threatened by advances in new technology. According to a recent Home Office study, the move to Internet Protocol (IP)-based communications will render the UK's domestic interception capability obsolete over the next decade. The Home Secretary told the Committee:

> *We do recognise the changing technology that we are facing, the way in which… both the collection and the dissemination of information and data will change fundamentally, and it will change more quickly in this country than it will in many others… The impact of that will be to massively degrade (unless we make big changes) our ability, not just to be able to intercept, but actually potentially to be able to collect the communications data in the first place in order to be able to target the interception.*[126]

175. This is a very complex issue but one that must be addressed as a matter of priority. In response, the Home Office has established the Interception Modernisation Programme, which aims to update how intelligence and law enforcement agencies collect and access communications data. On 15 October 2008, the Home Secretary announced that a public consultation would begin early in 2009 to inform Ministerial decisions as to any future legislation which might be necessary.

176. The Communications Data Bill – which had included a provision *"to ensure that public authorities can continue to have access to essential communications data"*[127] – is now on hold until the outcome of the public consultation next year.

Q. The Committee considers that maintaining the capability to intercept modern communications is of critical importance to the national security of the UK. We will be looking in detail at any forthcoming proposals.

Document security in the Cabinet Office

177. On 11 June 2008, it was widely reported in the media that top secret government papers originating from the JIC had been left on a train in London. These had been found by a member of the public who handed them to the BBC, which then contacted the police. This triggered both a police investigation and an internal Cabinet Office review of document security.

[126] *Oral evidence – Home Secretary, 5 February 2008.*

[127] *Letter from the Home Office, 27 June 2008.*

178. The Minister for the Cabinet Office made a statement to the House of Commons on 12 June 2008:

> *This was a clear breach of well established security rules that forbid the removal of documents of this kind outside secure government premises without clear authorisation and compliance with special security procedures… The Cabinet Secretary has asked Sir David Omand, former Permanent Secretary for Security and Intelligence… to carry out a full investigation of the circumstances of the case… I have asked Sir David to keep the Intelligence and Security Committee… fully informed.*[128]

179. The Cabinet Secretary set Sir David Omand the following terms of reference: to examine the circumstances which led to the loss of the papers, the procedures for the handling of such material, and whether any changes should be made to the existing arrangements for protecting highly classified papers in the Assessments Staff of the Cabinet Office.

180. The Committee wrote to Sir David Omand to draw his attention to the findings of an investigation into security arrangements in the Agencies that was commissioned by the Committee in 1999. One of the issues that concerned the Committee was the different arrangements relating to document security across the intelligence community. The investigation found that there are random exit searches in each of the Agencies, but that the Cabinet Office does not employ random searches, despite housing highly classified material in some areas.

181. Sir David wrote to the Committee on 14 July confirming that he had sent his provisional findings to the Cabinet Secretary. The Committee wrote to the Minister for the Cabinet Office requesting sight of these provisional findings. In response, on 4 August 2008, the Minister told the Committee that the review findings could not be made available until the Crown Prosecution Service had reached a view on prosecuting the individual involved.

182. On 28 October, the individual concerned[129] appeared before Westminster Magistrates' Court charged under Section 8.1[130] of the Official Secrets Act. He pleaded guilty and was fined £2,500 and ordered to pay court costs. At the time of writing,[131] the Committee is awaiting sight of Sir David's report.

[128] *HC Deb 12 June 2008 vol 477 cc 485–486.*

[129] *The individual in question was a member of the Assessments Staff in the Cabinet Office, on loan from the Ministry of Defence.*

[130] *Section 8.1 of the Official Secrets Act is concerned with the safeguarding of information.*

[131] *7 November 2008.*

Investigation into BAE Systems

183. In its 2006–2007 Annual Report, the Committee considered the intelligence and security matters that contributed to the Serious Fraud Office's (SFO's) decision to halt its investigation into allegations of financial irregularities in BAE Systems' dealings with the Saudi royal family. We reported that we were satisfied that, at that time, there were serious national security-related considerations that contributed to the SFO's decision. This remains the Committee's opinion.

184. In April 2008, a judicial review ruled that the SFO had acted unlawfully in halting its investigation. The SFO was subsequently granted leave to appeal this ruling and in July 2008 the House of Lords ruled that the SFO had acted lawfully in halting its investigation. This ruling overturned the High Court judgment. The judgment stated:

> *The issue in these proceedings is not whether his decision was right or wrong… but whether it was a decision which the Director was lawfully entitled to make… In the opinion of the House the Director's decision was one he was lawfully entitled to make. It may indeed be doubted whether a responsible decision-maker could, on the facts before the Director, have decided otherwise.*[132]

[132] *R. (on the application of Corner House Research and others) vs Director of the Serious Fraud Office [2008] UKHL 60, paragraphs 41 and 42, 30 July 2008.*

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

A. The work of the intelligence and security Agencies cannot be looked at in isolation and it remains essential that this Committee has oversight of the wider intelligence community.

B. We appreciate the challenge involved in retaining highly trained and specialist staff over the long term, and are encouraged by the steps that GCHQ has taken so far to deal with this problem.

C. It is reassuring that so few Security Service staff have felt the need to raise ethical concerns or complaints with the "Ethical Counsellor". We nevertheless welcome the establishment of the post and believe it provides an important avenue, should the need arise, for staff to discuss their concerns.

D. Whilst the Secret Intelligence Service has clearly recognised the wider emerging economic, political and military challenges, we are concerned that diverting resources to tackle the current terrorist threat means that such longer-term challenges might not be receiving adequate attention.

E. This is the second successive year that the Committee has raised concerns regarding the Secret Intelligence Service's policy on retirement age. We remain concerned that the Service's policy still does not seem fully to meet its business requirements. This should be dealt with as a matter of urgency.

F. Following the floods in the summer of 2007, the Agencies have reviewed and improved their business continuity and resilience planning. Whilst we are reassured by the work that has been done so far, and the further changes that are now being made, we consider that there is still scope for improvement.

G. Whilst the Committee recognises that a single budget ensures maximum flexibility for the Agencies to be able to respond to rapidly changing threats and events, we remain concerned that aspects of the Agencies' work that are not related to international counter-terrorism are continuing to suffer as a result of the focus on counter-terrorism.

H. The Committee welcomes the work being done to establish a new framework for monitoring the performance, efficiency and financial management of the Agencies. The Committee is also considering, in consultation with the Agencies, ways in which its oversight of the Agencies' budgets can be conducted in a more timely way.

I. The Committee welcomes the separation of the roles of Chairman of the Joint Intelligence Committee and the security adviser to the Prime Minister. We remain convinced, however, that for them to function effectively both posts must be at an appropriately senior grade.

J. Whilst the Committee welcomes the Cabinet Secretary's increased involvement in intelligence matters at a strategic level, we question the amount of time he can, in reality, give to his new line management role with the Agency Heads, in view of his other responsibilities. We will keep this arrangement under review.

K. Given the importance of the Professional Head of Intelligence Analysis (PHIA) post, we are very concerned by the plan to subsume the role within the Joint Intelligence Committee Chairman's post as this may actually lessen the priority given to this crucial role. The Committee is disappointed that the PHIA post has not been maintained as a distinct and separate role.

L. The Committee agrees that there is a need to improve understanding of "the path to extremism" and welcomes the establishment of a new team analysing open-source and academic material in this field. However, the team does not appear to sit comfortably within the Joint Terrorism Analysis Centre (JTAC). One of the key strengths of JTAC is its operational focus on the immediate threat from international terrorism – this should not be diluted in any way. Consideration should therefore be given to moving this new team to a more appropriate location (such as the Office for Security and Counter-Terrorism in the Home Office), with the establishment of a clear liaison function as necessary.

M. The Committee considers that the challenge process is vital to ensuring that the Joint Intelligence Committee product is of a good quality and must be encouraged.

N. We have consistently reported concerns about SCOPE and are appalled that Phase II of the system – on which tens of millions of pounds have been spent – has now had to be scrapped. We sincerely hope that lessons have been learnt from this failure and that they will be used when plans for the future are being drawn up. We also expect the development of any replacement capability to be subject to more stringent controls, and greater management and financial accountability, from the outset. We will be investigating the reasons for the serious failure of this important project, and will report on the matter in the forthcoming year.

O. The Defence Intelligence Staff (DIS) is a critical part of the UK intelligence community, and the single largest intelligence analytical capability in the UK. Its analysts are highly trained intelligence officers with a broad range of experience and knowledge who collectively make a critical contribution to the overall UK intelligence effort. Whilst the Committee understands that only 16% of DIS staff are based in Whitehall, it is, nevertheless, where its analysts are based, and therefore a cut in the number of Whitehall staff must mean a reduction in DIS's analytical capability. The Committee is therefore concerned by the possible impact on DIS's analytical capability of these efficiency savings and staff cuts, particularly when viewed against the very significant increases in resources that the Security Service, Secret Intelligence Service and GCHQ have received.

P. We welcome the fact that the Chilcot conditions meet our concerns that the Agencies' capability must not be damaged should their intercept material be adduced in court. We are concerned, however, as to whether it will be possible to meet these conditions.

Q. The Committee considers that maintaining the capability to intercept modern communications is of critical importance to the national security of the UK. We will be looking in detail at any forthcoming proposals.

LIST OF WITNESSES

Ministers

The Rt. Hon. Jacqui Smith MP – Home Secretary

The Rt. Hon. David Miliband MP – Foreign Secretary

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Sir David Pepper KCMG – Director, GCHQ (until 28 July 2008)

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Scarlett KCMG – Chief, SIS

Other officials

SECURITY SERVICE

Mr Jonathan Evans – Director General, Security Service

Other officials

CABINET OFFICE

Sir Gus O'Donnell KCB – Cabinet Secretary

Mr Robert Hannigan – Head, Intelligence, Security and Resilience

Mr Alex Allan – Chairman, Joint Intelligence Committee

Mr Chris Wright – Director, Security and Intelligence

Mr Tim Dowse – Chief, Assessments Staff

Dr Michael Taylor – SCOPE Programme Director

Other officials

MINISTRY OF DEFENCE

Air Marshal Stuart Peach – Chief, Defence Intelligence Staff

Other officials

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID6011184 02/09

Printed on paper containing 75% recycled fibre content minimum.

TSO
information & publishing solutions

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

Online
www.tsoshop.co.uk

Mail, Telephone Fax & E-mail
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: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

TSO Shops
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-175422-4

9 780101 754224