Intelligence and Security Committee

Annual Report 2008–2009

Chairman:
The Rt. Hon. Dr Kim Howells, MP

Intelligence and Security Committee

Annual Report 2008–2009

Chairman:

The Rt. Hon. Dr Kim Howells, MP

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
by Command of Her Majesty
March 2010

Cm 7807 £14.35

ISBN: 9780101780728

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

ID 2349429 03/10

Printed on paper containing 75% recycled fibre content minimum.

From: The Chairman, The Rt. Hon. Dr Kim Howells, MP

INTELLIGENCE AND SECURITY COMMITTEE

35 Great Smith Street, London SW1P 3BQ

ISC 2009/10/043 15 December 2009

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

Dear Prime Minister

I enclose the Intelligence and Security Committee's Annual Report for 2008–2009. This covers our work between December 2008, when we submitted our previous Annual Report, and July 2009.

The Committee has met on a total of 31 occasions during this time, taking oral and written evidence on the administration, policy and expenditure of the three security and intelligence Agencies, and investigating related matters across the wider intelligence community.

In addition to this Report, we have updated our review of the links between the CREVICE plotters and the 7 July bombers (published on 19 May 2009) and conducted an investigation into the policies and procedures that the Agencies follow with regard to contact with detainees (the subject of a separate report to you on 17 March 2009). This latter work will feed into the review we are now beginning – at your request – of the Agencies' consolidated guidance regarding the treatment and interviewing of detainees (which we received on 18 November 2009).

We hope that you will set a date to meet and discuss our findings as soon as possible, and that the Report can be published as soon as possible thereafter.

Yours

Kim

KIM HOWELLS

THE INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Dr Kim Howells, MP (Chairman)

The Rt. Hon. Michael Ancram QC, MP	*The Rt. Hon. George Howarth, MP*
The Rt. Hon. Sir Menzies Campbell CBE QC, MP	*The Rt. Hon. Michael Mates, MP*
Mr Ben Chapman, MP	*Mr Richard Ottaway, MP*
The Rt. Hon. Lord Foulkes of Cumnock	*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 the work of the Joint Intelligence Committee (JIC) and the Intelligence and Security Secretariat, which includes the Assessments Staff in the Cabinet Office. 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.

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. Under the terms of the Intelligence Services Act, material can be redacted if it is determined *"after consultation with the Committee, that the publication of any matter in a report would be prejudicial to the continued discharge of the functions of either of the Services or, as the case may be, GCHQ"*. This is indicated by *** in the text. To date, no material has been excluded without the Committee's consent.

CONTENTS

GLOSSARY

AGPC	Advisory Group of Privy Counsellors
CDI	Chief of Defence Intelligence
CIA	Central Intelligence Agency (US)
CIDT	Cruel, Inhuman or Degrading Treatment
CLiC	Collaboration in the Intelligence Community
CONTEST	UK Counter-Terrorism Strategy
CSR07	Comprehensive Spending Review 2007
CT	Counter-terrorism
DIS	Defence Intelligence Staff
DPBAC	Defence Press and Broadcasting Advisory Committee
FCO	Foreign and Commonwealth Office
GCHQ	Government Communications Headquarters
HFA	Hostile Foreign Activity
HMRC	Her Majesty's Revenue and Customs
HUMINT	Human-sourced Intelligence
IaE	Intercept as evidence
ICT	International Counter-terrorism
INOC	Internet Operations Centre
IONEC	Intelligence Officer New Entrants Course
ISC	Intelligence and Security Committee
JIC	Joint Intelligence Committee
JNAC	Joint Narcotics Analysis Centre
JTAC	Joint Terrorism Analysis Centre
MoD	Ministry of Defence
NDIST	Network Defence Intelligence and Security Team
NSID	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
SIA	Single Intelligence Account
SIGINT	Signals Intelligence
SIGMOD	GCHQ's SIGINT Modernisation Programme
SIS	Secret Intelligence Service
SOCA	Serious Organised Crime Agency
UKIMN	UK Intelligence Messaging Network

INTRODUCTION

1. This Report details the work of the Intelligence and Security Committee (ISC) for the period December 2008 to July 2009. The Committee has held 22 formal sessions and nine other meetings during this period.

2. The majority of the Committee's time during the reporting period was spent examining and taking 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.

3. The remainder of the Committee's time this year has been spent on two separate investigations:

- updating its *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*[1] to reflect developments since the review was originally sent to the Prime Minister on 8 July 2008. The completed review was published on 19 May 2009; and
- conducting an investigation – as a result of allegations surrounding the case of Binyam Mohamed al-Habashi – into the policies and procedures that the Agencies follow with regard to contact with detainees, and also intelligence sharing more widely. We wrote to the Prime Minister on 17 March 2009, reporting our findings.

We had intended to begin a review of the current UK intelligence and security Agencies' guidance regarding the treatment and interviewing of detainees. The Prime Minister wrote to the Committee on 18 March 2009 inviting the Committee to conduct this work, although the Committee did not receive the consolidated guidance documents during the period covered by this Report.[2]

4. In addition to its formal evidence sessions, the Committee has visited the Office for Security and Counter-Terrorism (OSCT) in the Home Office, the Security Service, the Joint Terrorism Analysis Centre (JTAC), the Secret Intelligence Service (SIS), the Cabinet Office Briefing Rooms and BBC Monitoring. As part of the Committee's programme of discussions with our overseas counterparts, we have held bilateral discussions with key officials and organisations in the US and Canadian intelligence communities and have hosted visitors from Spain, Canada, Singapore, Pakistan, Botswana, the US and Australia.

---

[1] *Cm 7617.*

[2] *The consolidated guidance was received on 18 November 2009.*

THE AGENCIES

The threat

5. The UK faces a range of covert threats to its security. The Security Service assesses the current level as follows:[3]

- There is a serious and sustained threat from international terrorism to the UK and UK interests overseas. The level during the period of this Report was assessed as 'Severe' (it was reduced to 'Substantial' on 20 July 2009). The most significant threat comes from al-Qaeda and associated networks.
- Northern Ireland-related terrorism continues to pose a threat. Dissident republican terrorist groups, who have rejected the 1998 Good Friday Agreement, still aspire to mount attacks in Northern Ireland and Great Britain.
- The proliferation of weapons of mass destruction poses potential danger to the UK's security.
- The threat from espionage remains high – several countries are actively seeking UK information and material to advance their own military, technological, political and economic programmes.

6. We cover the work that each of the UK intelligence and security Agencies is doing to counter these threats, and that posed by electronic attack (in which the Committee has a particular interest), in the following section.

The Single Intelligence Account[4]

7. In our last Annual Report we gave details of the resources allocated to the Agencies for the period 2008/09 to 2010/11 under the Comprehensive Spending Review 2007 (CSR07).[5] This increased funding available for the Agencies to just under £2 billion by 2010/11.

8. Although it is too early to speculate on funding in the post-CSR07 period, it is likely that the outlook for 2011/12 onwards will be very different, given the global economic downturn and the UK's current financial state.

A. The Committee considers it essential that the Agencies are able to consolidate the gains they have been able to achieve in recent years in terms of resources and capability. We would be concerned if the Agencies were to suffer real-term cuts in the short or medium term.

---

[3] *www.mi5.gov.uk.*

[4] *The financial data included in this Report is based on the Agencies' audited accounts for the financial year 2007/08 and all figures are at 2007/08 prices. For financial year 2008/09 onwards, the data is based on planned not actual expenditure.*

[5] *Cm 7542.*

9. Responsibility for the Agencies' finances lies with the Cabinet Secretary, as Principal Accounting Officer for the Single Intelligence Account (SIA). In addition, he has described himself as the Agencies' "Champion" on resources, a role that will be key as the Agencies approach the next Spending Round.[6] We asked the Cabinet Secretary how he was able to reconcile the two roles:

> *It is much easier for me to be a champion if I know that they are using their existing resources very efficiently and very well. In order to be a champion I need to be aware and make sure that they are doing that. If I felt they weren't doing well and there were serious underspends… it would certainly influence the way the Treasury approached new bids for money.*[7]

10. The Committee also questioned whether the Cabinet Secretary manages the SIA allocation between the Agencies or whether, in effect, the three individual budgets are distinct and fixed. It appears that there is limited flexibility:

> *[My] first call of action if, let's say, Jonathan Evans was to say to me he wants to spend more on counter-espionage in London, I would be saying reallocate your resources to do that. If it became a big issue and he said that is not possible, there would be that sort of conversation where we might think about do we move between Agencies.*[8]

We note, however, that the Cabinet Secretary only deals with the finances at a very strategic level, and that the day-to-day running of the SIA is undertaken by the Head of Intelligence, Security and Resilience at the Cabinet Office.

11. Last year we reported that the Cabinet Office and HM Treasury were working with the Agencies to develop a framework for monitoring efficiency and effectiveness across the Agencies, and that HM Treasury would be conducting a six-monthly stock-take of the Agencies' performance. We were subsequently told, in January 2009,[9] that:

> *Arrangements have been agreed with Treasury for SIA performance monitoring, the purpose of which is to demonstrate to the Principal Accounting Officer (PAO) and to the Treasury that resources are being used in an economical, effective and efficient manner. The aim of the arrangements is to:*
>
> *i. show accurately what has been spent across the SIA and give early warning of financial risks;*
>
> *ii. track performance in successfully delivering required outputs including efficiencies; and*
>
> *iii. show collectively that the SIA is fit for future purpose.*

---

[6] *The Cabinet Secretary is also the Line Manager of the Heads of the Agencies (as a result of the separation of the roles of Security Adviser to the Prime Minister and the Joint Intelligence Committee Chair). We have previously expressed reservations as to how much time the Cabinet Secretary is realistically able to devote to this role, given his other responsibilities.*

[7] *Oral evidence – Cabinet Secretary, 9 January 2009.*

[8] *Oral evidence – Cabinet Secretary, 9 January 2009.*

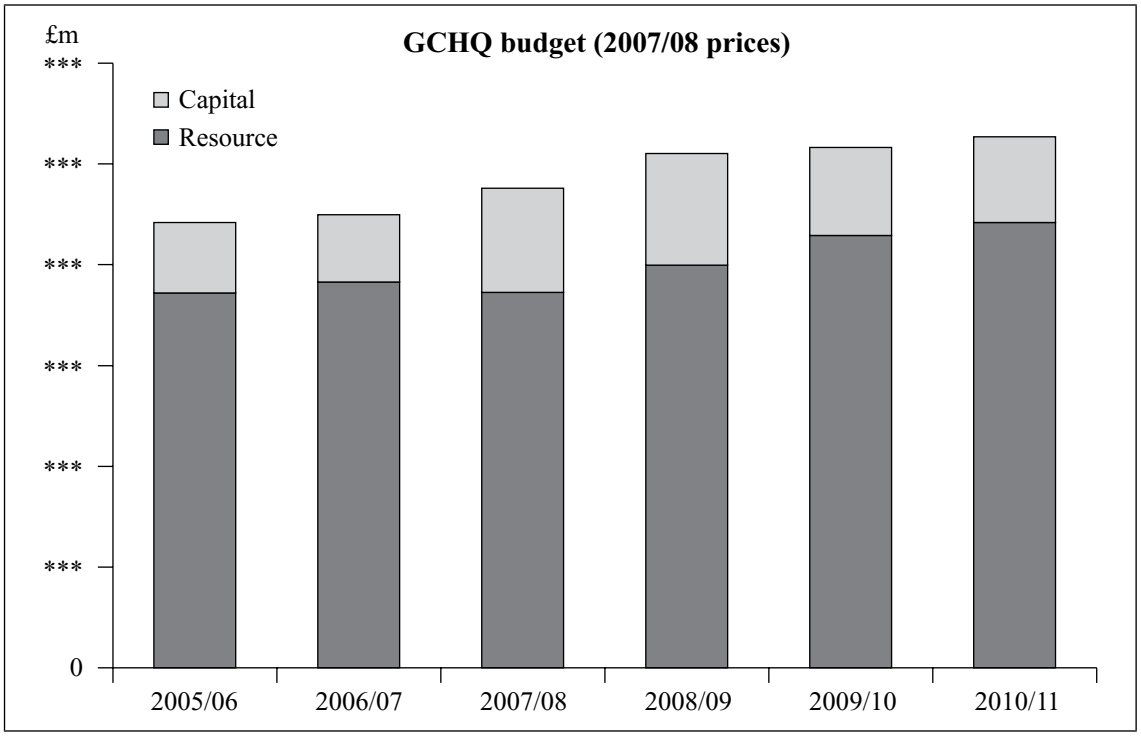
[9] *Letter from the Cabinet Office – 8 January 2009.*

12. When we asked for an update on how the new arrangements were working, we were informed that stock-takes were held in December 2008 and June 2009 which *"examined progress across the SIA on delivery of departmental strategic objectives, value for money, and the financial management of the Agencies, and have focused on ensuring that [the] Agencies continue to be able to deliver their CSR07 plans successfully"*.[10] We are pleased to note that these stock-takes are taking place, although we would expect to be kept updated on these as a matter of course in the future, rather than having to ask for information.

Government Communications Headquarters

Expenditure

13. The following chart demonstrates the growth in the Government Communications Headquarters' (GCHQ's) spending.[11]



14. GCHQ spent £*** million in 2007/08 (against a budget of £*** million). GCHQ's resource budget for 2008/09 was £*** million, which, added to a capital budget of £*** million, gave them a total budget of £*** million.[12] GCHQ's current spending priorities are to:

- sustain 2007/08 levels of investment;
- continue to invest in its internet-based capability; and
- maintain its support to international counter-terrorism (ICT) and UK military operations.

[10] *Written evidence – Cabinet Office, 17 June 2009.*

[11] *Actual spending for 2005/06 to 2007/08, and planned budgets to 2010/11.*

[12] *Net of £*** million PES (Public Expenditure Survey) transfer to the Ministry of Defence.*

15. We also reported in our 2007–2008 Annual Report on GCHQ's Signals Intelligence (SIGINT) Modernisation Programme (SIGMOD).[13] The major projects within the programme are: IT Infrastructure; Mastering the Internet; Better Analysis; and Support to Military Operations.

16. Given the very considerable funding required by SIGMOD (£*** million over the three financial years from 2007/08), and the sheer volume and complexity of the projects and contracts under the SIGMOD umbrella, effective financial oversight, project and contract management are critical. GCHQ has told the Committee that financial oversight is through GCHQ's twice-yearly Investment Board meetings, which review progress on major SIGMOD projects, supported by monthly internal management meetings to review progress more regularly. Procurement oversight is through the monthly Procurement Oversight Board (which is a formal sub-committee of the board). However, when questioned in detail on contract management, GCHQ admitted:

> *One of the critical weaknesses that has been flagged up for the last three or four years has been our whole approach to contract management… Historically [GCHQ] has not been as good at managing… contracts on an ongoing basis, hence that critical weakness.*[14]

GCHQ has now addressed this shortcoming by implementing a series of policy and process changes and recruiting three senior specialist contract managers.

B. It is essential that GCHQ's signals intelligence capability is maintained and indeed strengthened through its Signals Intelligence Modernisation Programme. However, given the considerable sums of money involved, it is also essential that the work is effectively overseen. We welcome the fact that GCHQ has now introduced improved contract management mechanisms.

17. In our 2006–2007 Annual Report[15] we reported that GCHQ had negotiated a deal (in February 2007) to repurchase its old Oakley site in order to address accommodation pressures. We have been told this year that accommodation problems remain, with the Benhall site now at full occupancy, and that GCHQ is examining a number of additional measures to find a cost-effective solution to this problem. We will report on this matter in more detail once GCHQ has evaluated the cost implications of the options available.

Policy

International counter-terrorism

18. GCHQ's work on counter-terrorism remained steady in 2007/08 at around a third of overall effort.[16] GCHQ's main focus is on the PURSUE strand of CONTEST, predominantly through support to the Security Service on counter-terrorism operations.

---

[13] *Cm 7542, page 11.*

[14] *Oral evidence – GCHQ, 24 February 2009.*

[15] *Cm 7299.*

[16] *The term "effort" relates to the amount of analytic and production resources dedicated to a particular task. It does not include other parts of GCHQ's work, some of which absorb considerable resources (such as SIGMOD), which will indirectly or in the longer term benefit its work on ICT.*

(A significant proportion of all the Security Service's counter-terrorism operations have benefited from GCHQ's initial lead information.)

19. Given the growth in the Security Service in recent years, and the resulting growth in the number of counter-terrorism operations, we asked GCHQ how it is coping with increasing demands for support. The Director of GCHQ told us:

> *We will take our lead from the Security Service in particular, if they are ranking the priorities. They will be under the same pressures and we will match their response. We will continue to look at targets where we believe we can produce intelligence, [including those] who may not be on that very top priority, but nevertheless could rise in priority.*[17]

C. The Committee had previously been told that it was "very unlikely" that GCHQ would ever be able to meet the performance targets agreed with the Security Service. We are therefore reassured that GCHQ now believes it is able to meet Security Service key requirements.

20. GCHQ staff are now integrated in Security Service and SIS Counter-Terrorism Teams, are seconded to the Joint Terrorism Analysis Centre, perform a liaison function with the Metropolitan Police Service's counter-terrorism work and are deployed overseas with the military: this represents genuine progress in collaborative working across the counter-terrorism community. The Director of GCHQ explained:

> *We've increased staff working on front-line CT analysis as planned and have deployed forward to partners, particularly to the Security Service and SIS. In the Security Service there is now a GCHQ presence in operational and investigative teams.*[18]

21. We have been briefed this year on GCHQ's increasing focus on the internet. The Director told the Committee:

> *We have increased the staff working to [combat] extremists' use of the internet; our research and development in that area is a real focus for us.*[19]

22. One aspect of this work is the Internet Operations Centre (INOC), which has now been in existence for two years. It brings together all of GCHQ's computer network operations capability in one team in support of internet-related counter-terrorism operations. The Committee has been told that the INOC has had some "proven successes".[20]

---

[17] *Oral evidence – GCHQ, 24 February 2009.*

[18] *Oral evidence – GCHQ, 24 February 2009.*

[19] *Oral evidence – GCHQ, 24 February 2009.*

[20] *For example, the Director of GCHQ explained that the INOC was able to provide *** intelligence regarding "*** ***". This intelligence was sent to UK customers and a range of foreign partners, including the *** authorities with whom GCHQ shared key elements in order to help head off any potential further attacks. (Oral evidence – GCHQ, 24 February 2009.)*

Non-ICT work

23. GCHQ continues to provide significant support to UK military forces overseas. In Iraq, the focus has shifted from direct support to UK military operations towards providing SIGINT in support of areas of strategic importance. Support to UK forces in Afghanistan continues to be a major part of GCHQ's effort, in terms of both support to operations and strategic intelligence gathering, with plans for this to increase during 2009/10.

24. The Committee has questioned GCHQ this year on the threat of electronic attacks against both government and private sector IT networks. The Director of GCHQ outlined the nature of this threat:

> *The greatest threat is from state actors and there is an increasing vulnerability, as the critical national infrastructure and other networks become more interdependent.*[21]

25. State-sponsored electronic attack is increasingly being used by nations to gather intelligence, particularly when more traditional espionage methods cannot be used. It is assessed that the greatest threat of such attacks against the UK comes from China and Russia.[22] The Centre for the Protection of National Infrastructure (CPNI) told the Committee:

i. Foreign intelligence services conduct large-scale electronic attacks with the aim of stealing government, defence and technology information from targets in both government and industry. The Committee has been told that most large UK companies will have been targeted to some extent and that, in many cases, attacks against targets in the defence and technology sectors have been successful.

ii. Electronic attack is also used by Islamist terrorists who have the capability to launch limited forms of attack over the internet. Technical capability varies greatly, and it appears that their intentions are the defacement or denial of service of specific websites. These attempts are often ***. There are, however, indications that awareness and use of electronic attack is on the increase and ***.

26. In response to this threat, GCHQ created the Network Defence Intelligence and Security Team (NDIST) in September 2008, integrating its *** work to provide co-ordinated advice to government.[23] This provides customers with a service of detection, analysis, reporting and investigation of electronic attacks. The Committee has been told that NDIST has already demonstrated a number of tangible benefits, both in terms of practical emergency responses for government networks and developing a better understanding of the future threat.

27. Nevertheless, work to tackle the threat of electronic attack is about a third below the level planned. We have been told that the shortfall is because of the difficulties GCHQ has had in recruiting and retaining skilled internet specialists in sufficient numbers – although specialist recruitment campaigns have been set up to try and address this problem.

---

[21] *Oral evidence – GCHQ, 24 February 2009.*

[22] *Written evidence – CPNI, 4 June 2009.*

[23] *There is also generic work to counter the threat of electronic attack being carried out within SIGMOD.*

D. The potential threat posed to the UK Government, critical national infrastructure and commercial companies from electronic attack is a matter for concern. We have heard from our American and Canadian counterparts that they treat this threat very seriously, and we recommend that the UK accord it a similar priority and resources.

28. On 25 June 2009 the Cabinet Office published a paper entitled: *The Cyber Security Strategy for the United Kingdom: Safety, Security and Resilience in Cyber Space*.[24] The strategy includes the formation of two new organisations: the UK Office of Cyber Security – which will be hosted initially by the Cabinet Office – and the UK Cyber Security Operations Centre, to be based at GCHQ in Cheltenham. Both of these organisations will be established in September 2009 and operational by the end of March 2010. This is a notable development in an area of work of considerable interest to the Committee. We were therefore disappointed not to have been given sufficient notification to have been able to include any further assessment of the strategy in this Report.

Administration

29. GCHQ recruited 410 new staff in 2007/08 against its target of 660. Talking about the shortfall, the Director of GCHQ said:

> *It is hard to find [specialist staff] from outside… It's very difficult because I think the individuals may not be out there. We may have to grow some of them, and I think we have to encourage industry to grow some of them… We are partnering with six key relatively well-off companies within the IT sector.*[25]

30. Despite the difficulties experienced in previous years, the recruitment target for 2008/09 is even more ambitious, requiring 750 additional new staff. To try to meet this, GCHQ has explored new recruitment strategies – including the use of video boards on London Underground and mass marketing along commuter routes into London, as well as dedicated websites. These strategies are aimed at attracting internet specialists, those with particular language skills, and technologists.

31. In our 2007–2008 Annual Report we reported the difficulties experienced by GCHQ in retaining specialist staff. This year GCHQ told us that, while the recruitment of highly specialised staff remains a challenge, the retention of existing staff has improved:

> *There's no major issue in the last 12 months about losses of specific technical skills… the deterioration in the economic situation is actually making recruiting slightly more straightforward.*[26]

Laptops unaccounted for

32. The National Audit Office management letter, reporting on GCHQ's 2007/08 accounts, criticised the results of GCHQ's 2008 laptop computer audit. This showed that 35 laptops were unaccounted for, including three that were certified to hold Top

---

[24] *Cm 7642.*

[25] *Oral evidence – GCHQ, 24 February 2009.*

[26] *Oral evidence – GCHQ, 24 February 2009.*

Secret information; the rest were unclassified.[27] We pressed GCHQ about its procedures for controlling and tracking such equipment. It appears that the process for logging the allocation and subsequent location of laptops has been haphazard. We were told:

> *Historically, we just checked them in and checked them out and updated the records when they went through our… laptop control process.*[28]

33. The Director explained that the rapid deployment of both personnel and assets had compounded the problems:

> *A lot of the laptops are shipped out to sites either in the theatres of war for communications means or to control equipment and… against an operational imperative, I think perhaps some people perhaps took slightly hasty decisions without due process.*[29]

34. Whatever the precise circumstances in which the laptops went missing, GCHQ recognises that its control processes were still not sufficiently robust:

> *Not only do we need to check them when they [laptops] are moving in and out of the building, but at a particular point in the year we are going to check to say we know exactly where every single one is.*[30]

35. As a result, GCHQ has reviewed its policies and has put new procedures in place, which comply with the new mandatory standards for the handling of data across government. This includes an annual audit of laptops and their location. The Director informed us that:

> *We now believe that we have the records for this recent period for our current holdings and that we can now… know who holds the laptops and who has drawn a laptop from a pool.*[31]

E. The Committee considers that this formerly cavalier attitude towards valuable and sensitive assets was unacceptable. GCHQ must ensure that it controls, tracks and monitors its equipment effectively. Now that proper processes have been introduced, we trust that this problem will not arise again.

---

[27] *We were informed that seven of these had been located (as at February 2009) and a further ten had been sent for destruction. GCHQ says that there is no evidence of any loss of classified information and that the risk remains low given the time that has elapsed (they went missing prior to 2005).*

[28] *Oral evidence – GCHQ, 24 February 2009.*

[29] *Oral evidence – GCHQ, 24 February 2009.*

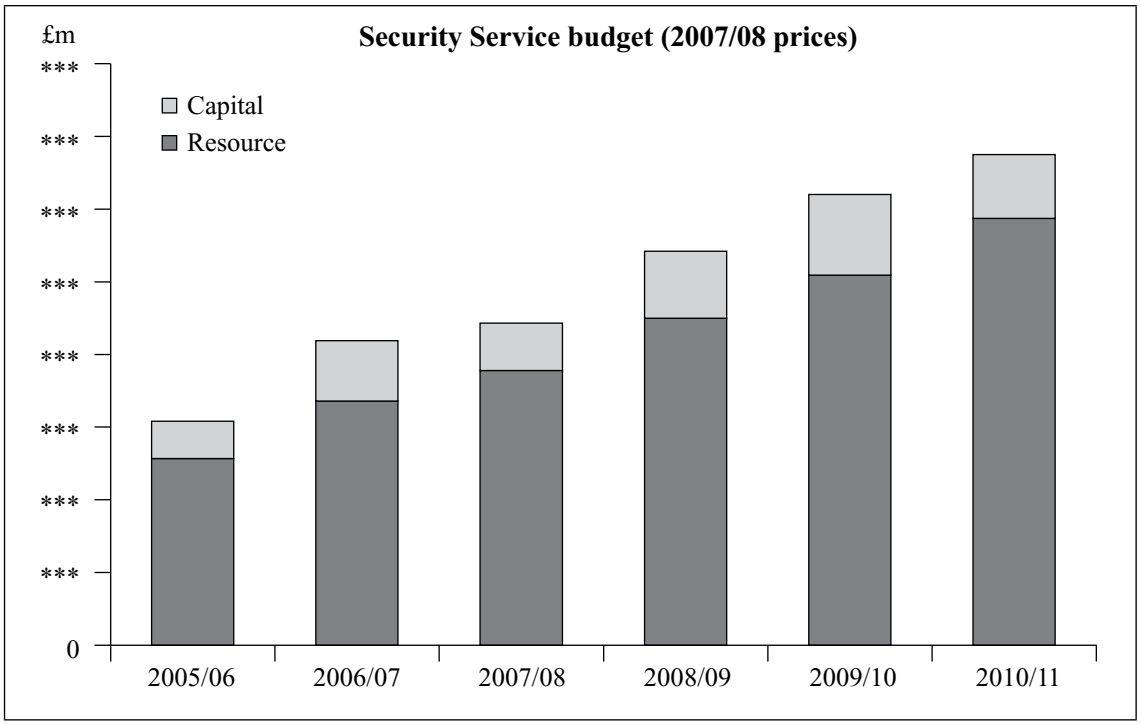
[30] *Oral evidence – GCHQ, 24 February 2009.*

[31] *Oral evidence – GCHQ, 24 February 2009.*

The Security Service

Expenditure

36. The following chart demonstrates the growth in the Security Service's spending.[32]



37. Security Service total spending increased to £*** million in 2007/08 (against a budget of £*** million), compared with £*** million in 2006/07.[33] Capital spending in 2007/08 dropped to £*** million.[34] During 2007/08, the Security Service completed two major capital projects:

- the Northern Operations Centre – costing a total of £*** million over a three-year period; and
- refurbishment of additional London accommodation – costing a total of £*** million.

38. The Service received a good settlement for the period covering 2008 to 2011, which will allow it to consolidate earlier growth and fund new investment in infrastructure and technology projects. The Director General explained the importance of the Service developing its technological capability:

> *Our targets are increasingly using computers rather than telephones *** ***.*[35]

---

[32] *Actual spending for 2005/06 to 2007/08, and planned budgets to 2010/11.*

[33] *The Security Service Resource Account was agreed by the Comptroller and Auditor General in October 2008.*

[34] *This is a reduction from a figure of £*** million in 2006/07 – this was due to a number of key technical and accommodation projects having been completed, and included the sum of £*** million on the Service's new building in Northern Ireland.*

[35] *Oral evidence – Security Service, 10 February 2009.*

39. In addition, key areas in which the Service plans to invest over the CSR period include:

- further recruitment, to bring total staffing up to around 4,100;[36]
- focusing on consolidating its regional network;[37]
- increasing the capacity of its computer data centre with the addition of four data halls; and
- development of corporate IT systems to enable the transformation of desktop IT, regional connectivity and business resilience.

Policy

International counter-terrorism

40. The Security Service allocated 67% of its resources to ICT over 2007/08. This is expected to increase to 75% in 2008/09.

41. Although the assessment of the level of threat from international terrorism was reduced on 20 July 2009, 'Substantial' is still a high level of threat and the Security Service continues to investigate a large number of targets of interest. While the overall number of individuals on the Service's database associated with Islamist extremist terrorism will vary from week to week, the total has not changed greatly for some time. The UK remains a key potential target for such individuals. The Committee has been told that, as at the beginning of July 2009, there were just under 200 major investigations, over 15% of which represented a high level of threat.

42. Nevertheless, the Director General told us that the level of "late stage" attack planning in the UK it is discovering is currently lower than the Service has seen in previous years:

> *We have been giving quite a lot of thought as to why that is. It's not because the people aren't here, because they very clearly are and we believe their strategic intent is the same, but I think there are a number of factors in play. One is the very large number of cases that have come through the courts and been successfully prosecuted by the CPS [Crown Prosecution Service], which has an effect on the willingness of groups to take risks and to do things. Secondly, I think there has been a degree of disruption, particularly in the FATA [Federally Administered Tribal Areas].*[38]

43. The security threat is changing in other ways too: although threats linked to Pakistan remain the primary area of concern, about 15% of the Security Service's work now relates to East Africa, and Somalia in particular, with a number of extremists visiting that country for training purposes.[39]

---

[36] *We have since been informed that this target has been reduced to 3,800.*

[37] *Regional stations in the South East, East Midlands and West Midlands were opened during 2008/09 and a station in the Thames Valley is planned to open in late 2009.*

[38] *Oral evidence – Security Service, 10 February 2009.*

[39] *Oral evidence – Security Service, 10 February 2009.*

Non-ICT work

Northern Ireland-related terrorism

44. The Government's Independent Reviewer of Terrorism Legislation (Lord Carlile of Berriew) completed his first review of national security arrangements in Northern Ireland in October 2008. His report noted that the transfer of responsibility from the Police Service of Northern Ireland (PSNI) to the Security Service had been successful, with no deterioration in national security coverage as a result of the transfer.

45. Last year we reported that, although a threat remained, the overall threat from Northern Ireland-related terrorism had diminished in recent years and that the Security Service had made an adjustment in its allocation of resources: from 17% in 2006/07 to 15% in 2007/08.[40] However, by October 2008, the increase in dissident republican activity meant that the planning assumptions had to be revised. Giving evidence to the Committee in February 2009, the Director General observed:

> *We are quite worried about both the events and the intelligence in Northern Ireland. Since the summer of last year, [we've] had to reinforce in Northern Ireland in order to keep ourselves in a position where we had a reasonable prospect of being able to stop planned attacks.*[41]

46. The intelligence picture in Northern Ireland prompted the raising of the dissident republican terrorist threat level from "Substantial" (an attack is a strong possibility) to "Severe" (an attack is highly likely). The Director General wrote to the Committee on 25 February 2009 to inform us that this decision followed:

> *A period of sustained activity by dissident republican groups, who continue to plan attacks, principally focused on killing members of the police, and who show increasing capability in so doing.*[42]

47. These concerns were borne out the following month, when two separate terrorist attacks took place. On Saturday 7 March 2009, two soldiers from 38 Engineer Regiment were killed in an attack on Massereene Barracks in Antrim. Two days later a PSNI Constable was murdered in Craigavon, County Armagh on Monday 9 March 2009.

F. The attacks in Northern Ireland in March 2009 have shown that the threat from dissident republican terrorism remains very real. While the overall intelligence assessment was accurate, and the threat level was at an appropriate level, *.**

Counter-espionage

48. The allocation of effort on countering hostile foreign activity (HFA) fell in 2007/08, from approximately £*** million in 2006/07 to under £*** million. In 2008/09 it is planned that the resources dedicated to this work will remain relatively constant at around £*** million.

---

[40] *Cm 7542, page 17.*

[41] *Oral evidence – Security Service, 10 February 2009.*

[42] *Letter from the Security Service – 25 February 2009.*

49. *** continues to be a focus, and in particular the activities of the *** intelligence services in the UK.[43] The Director General acknowledged that the Service needs:

> *Better insight into that rather complex web of relationships between ***… which has quite a significant presence in the UK. I don't think, at the moment, we have as much insight into that as I would like to have in order to be able to give sensible advice to government on the significance of that in security terms.*[44]

With regard to ***, the Director General informed us that:

> *We are concerned about ***, particularly electronic attack, although not only electronic attack, although we see less *** activity here than is seen in other countries.*[45]

50. When asked by the Committee if any consideration had been given to ring-fencing a proportion of the budget, the Director General acknowledged:

> *I would like to do more on HFA, because I think there are unanswered questions out there and ones which are slow-burn rather than rapid problems, and if you ignore them for long enough they are likely to cause us problems. So I would like to increase it… at the end of the day, if you are in Operation OVERT or something, with a huge terrorism plot, you will forget any surveillance for *** because you've got to throw everything at the major problem at hand. Therefore I don't want to ring-fence our operational resource to any particular area, because it seems to me it has to go where the operational demand is that day, and it's very flexible and we can change it around by lunchtime if we need to.*[46]

G. We accept the view of the Security Service that ring-fenced funding would limit its operational flexibility. However, as we stated last year, we are still concerned that counter-espionage is not sufficiently resourced in light of the levels of hostile foreign activity in the United Kingdom. This is a serious threat that must not be overlooked.

Administration

51. The Security Service has continued its rapid recruitment programme and plans to grow to around 4,100 staff by the end of 2010/11 (compared with current staffing of approximately 3,500).[47]

52. Although staff numbers are increasing, there has been a significant shift in the focus of recruitment this year: the Service has been increasingly seeking more specialists, such as those with IT skills.

---

[43] *Cm 7542.*

[44] *Oral evidence – Security Service, 10 February 2009.*

[45] *Oral evidence – Security Service, 10 February 2009.*

[46] *Oral evidence – Security Service, 10 February 2009.*

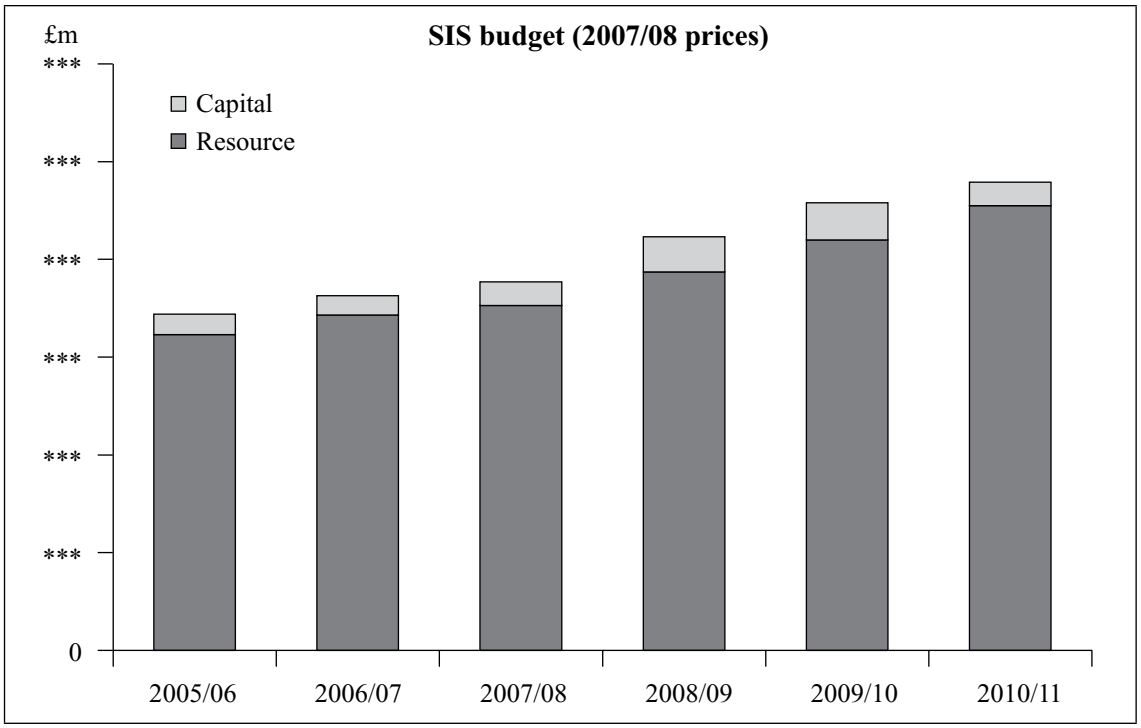
[47] *We have since been informed that this target has been reduced to 3,800.*

53. The Service has attributed the success of its recruitment campaigns to a focus on raising awareness of the Security Service as an employer of choice, with radio commercials and a media advertising campaign aimed at London commuters. It also broadened the scope of its online testing, which is providing significant time and cost savings at the initial stages of the recruitment process. Screening mechanisms have been improved so that candidates with serious vetting concerns can be identified and rejected at an early stage.

The Secret Intelligence Service

Expenditure

54. The following chart demonstrates the growth in the Secret Intelligence Service's (SIS's) spending.[48]



55. SIS spent £*** million resource in 2007/08 (against a budget of £*** million), an increase of 5.5% over the previous year. Capital spending for 2007/08 was £*** million. However, nearly a third of this was spent in the last month of the financial year, despite a previous National Audit Office recommendation that SIS improves its financial planning systems in order to avoid such last-minute surges.

H. This is the second year in a row that the Secret Intelligence Service has failed to manage its capital spend across the financial year, putting both efficiency gains and value-for-money gains at risk.

[48] *Actual spending for 2005/06 to 2007/08, and planned budgets to 2010/11.*

56. SIS has now appointed a senior official to manage IT budgets across the Service, an area where this kind of expenditure surge has been particularly prevalent. We hope that this appointment will help the department to plan more effectively and organise capital spending across the year.

57. SIS's initial budget for 2008/09 is £*** million resource and £*** million for capital projects. These increases will be spent primarily in three areas:

- growth in staff numbers (particularly overseas), with an extra *** operational posts between 2008 and 2010;
- updating and making better use of existing accommodation; and
- continued investment in the *** programme to connect SIS stations and offices, allowing secure access to highly classified information across the world.

Policy

International Counter-terrorism

58. SIS devoted just over 33% of total effort in 2007/08 to counter-terrorism work, increasing to nearly 37% in 2008/09. Despite the greater level of resources being dedicated to ICT work, the Chief of SIS told the Committee that there remained major challenges:

> *The need to maintain our effort against the more sophisticated political targets in the counter-terrorism environment… gets more and more demanding and more and more complicated.*[49]

59. The Chief of SIS also explained that:

> *The key measure of success for us is to what extent it is promoting our ability to conduct our work upstream…*** *the hardest parts* *** *and related planning activity… mainly…*****. *We still haven't fully realised the potential which is there through our joint work across the country and getting resources upstream.*[50]

Non-ICT work

60. SIS devoted just over ***% of effort towards Russia during 2007/08 (*** the previous year) and planned to devote ***% during 2008/09. SIS reported that it produced *** on Russia in ***, largely as a result of maintaining its expertise in this area: *"So we have *** on Russia ***."*

61. We reported last year that SIS had been seeking to increase its effort dedicated to *** in order to manage the intelligence requirements arising from the challenge of ***, but that these expansion plans had had to be delayed as a result of ICT work being prioritised. Effort against *** during 2007/08 has therefore remained at just over ***%. The Chief of SIS told us:

---

[49] *Oral evidence – SIS, 27 January 2009.*

[50] *Oral evidence – SIS, 27 January 2009.*

*Until we get the numbers through towards the end of the spending round period, the resources simply aren't there to make a massive increase on ***… Without doubt this is where I want to continue to improve our investment… We have invested more and we have produced some pretty good results, but it needs to be better.*[51]

I. The Committee remains concerned that work to address this important challenge is not being adequately resourced.

62. SIS has also contributed to the Government's understanding of the current global financial crisis, including the implications of the crisis in key countries such as *** and ***, and providing intelligence on the impact of the crisis on countries threatened by the economic downturn, whose stability is important to UK national interests (e.g. ***).

Administration

Staffing

63. SIS recruited 204 new staff during 2007/08, against a target of 230 (the remainder having been selected but had not yet started). As at 31 March 2009, SIS had 2,253 staff; this is predicted to increase to 2,527 by March 2010.

64. Last year we noted SIS's plans to increase overseas deployments by around 40%, strengthening existing stations and creating new stations in order to enhance its global reach. However, this year the Chief told the Committee that this has not progressed as planned:

We increased our overseas deployments within the CSR07 period… as quickly but also as safely as possible. It has so far been slower than we had hoped or planned.[52]

When asked why deployments had not increased as planned, the Chief explained that there were two key problems:

i. changes in the nature of overseas deployment; and

ii. the change in the demographic pattern of the Service.

65. On the first point, the Chief explained that, as conditions in overseas postings became more difficult, SIS was having to adapt its standard arrangements and this was proving both complicated and expensive. He cited *** as an example:

*[Officers in] ****
*****... Well, we have quite a large number of operational officers at their peak, in their peak operational case officer years, who ***, and so on, who have gone out on ***... So (a) we have to give them more leave, (b) we have to shorten their postings, and (c) we are giving them the possibility to ****
*****… That is tricky… but if we don't do it we won't be able to deploy the numbers of really good people that we need to deploy to a place like that.*

[51] *Oral evidence – SIS, 27 January 2009.*
[52] *Oral evidence – SIS, 27 January 2009.*

66. On the second point, the Chief explained that, due to the time taken to train new staff, and the time required for them to accumulate sufficient experience, the recent rise in staff numbers had yet to result in any real increase in terms of the numbers of staff who were actually deployable. As a result, SIS has reviewed its training arrangements and the Intelligence Officer New Entrants Course (IONEC), which was previously open only to Intelligence Officers and took six months, has been redesigned into two three-month modules open to a wider group of staff.[53] SIS hopes that this will allow for the speedier deployment of new entrants into operational jobs and provide greater flexibility in terms of providing a greater number of staff who can do a wider range of jobs.[54]

67. The Committee asked when the Chief expected to be able to achieve a step change in overseas deployment and was told that results should be beginning to be seen from the second half of 2009 onwards, and that the eventual target was *"well over *** extra deployed posts overseas by March 2011"*.[55]

J. While the Secret Intelligence Service has made a step change in recent years in terms of staff numbers, the benefits have yet to be seen in terms of an increase in operational capability. It has recognised the need to adapt its established procedures – for example on terms of overseas deployment and training of new entrants – and we hope that this will begin to yield results soon.

Information management

68. With the significant growth in staff numbers in recent years, as previously mentioned, SIS now has a higher proportion of younger and less experienced officers. This carries significant risk – one of the keys to managing this is ensuring that officers without sufficient experience can at least have access to the existing knowledge and expertise within the organisation.[56] However, SIS has itself recognised that its existing systems are not as good as they should be. The Chief of SIS told us:

> *Managing the bulk data we now obtain is an important new policy and reputational issue for us… Making the right information and knowledge available to the right people at the right time and ensuring its accuracy is a crucial component. The risk of "not knowing what we know" has been recognised for some time, principally in CT. At a less exalted but still very important level, failures properly to exploit tribal knowledge and information in SIS continue to contribute significantly to operational errors.*[57]

69. The ability to manage information effectively is crucial to an organisation such as SIS, given the nature of its work. Recognising the importance of this issue, the Chief of SIS has appointed a senior officer as responsible for ensuring that shortcomings in the Service's information management are addressed and improvements made. Key to this is

---

[53] *The Committee visited SIS's training facility, in December 2008, to see how the new course was running (and took part in one of the training sessions).*

[54] *The Committee has been reassured that the benefits of the full IONEC are still being delivered to the Intelligence Officer cadre, but now in two separate courses, which provides more flexibility in terms of their deployment.*

[55] *SIS's most recent assessment is that up to *** such posts will be established by this date, with the remainder to follow in 2011/12.*

[56] *Record keeping across the Agencies is discussed in paragraphs 159 to 165.*

[57] *Letter from SIS – 10 November 2008.*

the *** programme, which aims to provide SIS staff, both UK-based and those operating overseas, with timely and reliable access to classified information. The Committee has been told that benefits will include:

- strengthening intelligence collection and covert action capability by enabling more secure operations through much wider access to key information;
- achieving faster operational results by ensuring access to the right information at the right time; and
- reducing operational risks to officers and agents through the better use of available information.

eBay sale of digital camera containing SIS data

70. On 30 September 2008, *The Sun* newspaper reported that SIS data had been contained on the memory stick of a camera purchased on eBay, the online auction site. The Committee questioned SIS about this matter, and was told that SIS had been alerted on 18 September that a member of the public had voluntarily handed in to Hertfordshire Special Branch a memory stick containing images of documents and photographs, some of which were highly classified. SIS completed an internal investigation before referring the case formally to the Metropolitan Police Service on 30 September. The police were firstly concerned with the security of the classified material, and that all electronic copies had been destroyed or were under their control.[58] The police determined that *** the camera storage media at around the time it went missing from the SIS station in *** in early 2004. *** the SIS station at the time.

71. SIS advised the Committee that its IT and communications system in *** at that time required files (including scanned documents and other images) to be transferred via floppy disk. Staff found that it was possible to use the station's digital cameras, rather than floppy disks, to transfer larger files – even though this was a breach of security operating procedures – and this is how this data came to be stored on the camera memory stick.

72. Once the memory stick had been used to store such highly classified information, it should have been:

- labelled clearly to show the classification of the data (it was not);
- held securely in the station (it was not); and
- destroyed according to normal security procedures (it was not).

As a direct consequence of the camera and memory stick not being properly labelled, it appears that the classified nature of the camera and its contents were forgotten, and the ***.

[58] *Letter from SIS – 2 October 2008.*

73. The Committee was informed on 1 April 2009 that SIS had concluded that the ***, transportation and subsequent sale of the camera (which belonged to SIS), the memory stick and the data contained on it were a genuine mistake and there was no malicious intent on the part of those involved. Having completed its investigation and interviewed everyone involved, the Metropolitan Police Service concluded that there was no evidence to support the referral of the case to the Crown Prosecution Service.

74. SIS has told the Committee that security policies and procedures have tightened considerably since 2003. Since this incident it has reviewed its policy and procedures for the handling of electronic media within the Service – both for SIS staff and for seconded staff and contractors.

K. The loss of Secret Intelligence Service data and its subsequent appearance on eBay represents a clear breach of data security procedures, combined with a lack of adequate guidance and enforcement. Although this happened some years ago, the Committee is nonetheless disappointed that data was not being handled securely.

CROSS-CUTTING ISSUES

Business continuity

75. In our 2007–2008 Annual Report we reported on the business continuity arrangements of all three Agencies and concluded that there was still scope for improvement. We have therefore returned to the issue this year to see if the proposed changes have been implemented.

GCHQ

76. Improvements over the past year have included the consolidation of IT infrastructure into computer halls *** which has improved resilience. However, key operational equipment remains centred around Cheltenham, which means that vulnerabilities remain. The Director acknowledges that this is not sensible in the long term and is exploring possible solutions.

77. The Committee has been briefed on plans for a new "data centre" to act as a back-up site ***:[59]

> *In SR07 we didn't bid for the funds to do a new resilient facility. So we have done the initial study with the other two Agencies and that came back with a costing of about £*** million to £*** million. Prior to that GCHQ had done its own independent study on building a resilient data centre for itself and the prices were in that same sort of ballpark. As a result of those pieces of costing work, the three Agencies have concluded that none of the three of us have the funding within our baselines to pay that sort of bill. So we will be attempting to make the case in the next spending review to obtain the funding to do that.*[60]

The Security Service

78. Last year the Director General told us that there were concerns about the resilience of Security Service IT networks and a lack of testing of business continuity plans generally. This year, the Director General told us that there had been improvements in IT resilience, but that serious risks remain:

> *Although we are just completing a ***, which is ***, best practice would suggest that you ***. So that's a longer-term ambition.*[61]

79. The Committee has also asked about business continuity more generally and was told *"the [international counter-terrorism] fall-back plan is not yet completely delivered, and has not yet been thoroughly tested"*.[62] The Security Service explained that, since its plans were based on moving large numbers of staff around, *"considerable planning*

---

[59] *We have been told that *** is a possible location.*

[60] *Oral evidence – GCHQ, 24 January 2009.*

[61] *Oral evidence – Security Service, 10 February 2009.*

[62] *Letter from the Security Service – 24 October 2008.*

and co-ordination is required to avoid excessive disruption to normal business".[63] The Committee recognises that the Service must minimise the risk to day-to-day working, but it is difficult to have confidence in any plan that has yet to be fully tested.

80. We were informed that the Security Service Management Board had agreed in April that priority for 2009/10 would be given to:

- improving assurance through technical testing of business continuity;
- training to improve IT systems' recovery times post-incident; and
- technical investigations into improving capability to revert IT systems from ***.[64]

The Secret Intelligence Service

81. The Committee has been told that SIS regularly tests the IT support infrastructure at its backup site and occasionally tests how teams would work away from SIS Head Office. Actual evacuation between its headquarters and the primary backup site is not practised and, moreover, there is no provision *** that site in the event that any incident ***.[65]

82. In our two previous Annual Reports, we have noted concerns about SIS's data backup procedures.[66] SIS has informed the Committee that the bulk of SIS's main systems are now replicated at the primary backup site and tested at least annually. Work is also continuing in the short to medium term to improve the Service's disaster recovery arrangements, including communication with overseas stations and for payment of staff.[67] However, at present:

> *Backup data for these systems continues to be ***. This has *** to ensure that the risk of interception is minimised. Even if the data were to be intercepted, SIS do not consider that a hostile government could make use of it without ***.*[68]

83. The Service is considering introducing a secure remote backup solution via a dedicated encrypted link that will enable more regular, secure and straightforward data transfer between its main data storage site and the backup site. However, due to other priorities, this is unlikely to be in place in the foreseeable future. The Committee remains concerned that, in the meantime, SIS's data backup arrangements are inadequate.

Conclusion

L. Effective and regularly tested business continuity plans are essential for all organisations. We recognise that progress is being made, but remain concerned that there are still vulnerabilities in the plans of all three Agencies. We shall examine these further.

---

[63] *Letter from the Security Service – 20 May 2009.*

[64] *Letter from the Security Service – 20 May 2009.*

[65] *There are plans to request the Ministry of Defence to assist with ***, but this is currently under negotiation.*

[66] *Cm 7299 and Cm 7542.*

[67] *Letter from SIS – 22 May 2009.*

[68] *Letter from SIS – 22 May 2009.*

Media relations

84. In our 2006–2007 Annual Report we reported our concerns – based on those voiced to us by the Cabinet Secretary and also the then Director General of the Security Service – that there was an increasing number of inaccurate and misleading reports in the media relating to the work of the intelligence and security Agencies, and regarding the reporting of leaked and sensitive intelligence. We concluded that the DA-Notice system – designed to protect information that, if it were published, would damage national security – was not working as effectively as it might.[69]

85. A year later, just prior to the publication of our 2007–2008 Annual Report, the Committee was itself the subject of just such an inaccurate and misleading report. *The Independent* carried a wholly erroneous story on its front page, alleging that we would recommend the introduction of legally binding powers to ban the media from reporting matters of national security. This story had no factual basis whatsoever. However, shortly afterwards, the Vice-Chair, and Chair of the Media Side, of the Defence Press and Broadcasting Advisory Committee (DPBAC) (currently Simon Bucks, Associate Editor of Sky News) wrote to us to set out the concerns of the Media Side about the Committee making any such recommendation.

86. We met Sir Bill Jeffrey, the Permanent Under Secretary at the Ministry of Defence and the Chair of the DPBAC, Simon Bucks, the Vice-Chair of the DPBAC and the Chair of the Media Side of the Committee, and Air Vice-Marshal Andrew Vallance, the Secretary to the Committee, to discuss the work of the DPBAC. They were keen that the Committee was aware of their work, with one such example being the recent case of the intelligence documents that were left on a train by a member of the Cabinet Office Assessments Staff:

> *When the BBC drew to [the Secretary's] attention the fact that these documents had been handed to them, there was an agreement reached that they would report the fact that the documents had been lost and the titles of them, but the BBC agreed that they wouldn't publish any part of the contents of them, or identify at that stage at least the official concerned.*[70]

87. They also said that the DPBAC was a "dynamic" organisation that kept the Notices under constant review, and the expansion of DA-Notice 5 to cover the activities of the Serious Organised Crime Agency (SOCA) was cited as an example (although we note that this in itself took 18 months).

88. We recognise that the freedom of the media to report on what it wishes is a fundamental principle in a democratic society: we have never sought to recommend any bans on reporting. Nevertheless the fact remains that, despite all that the DPBAC does, even Sir Bill Jeffrey himself said: *"I don't want to overstate the effectiveness of this machinery."*[71]

---

[69] *Following this report, we received representations from the Chair of the Media Side of the Defence Press and Broadcasting Advisory Committee. It was clear that he believed that we were insufficiently aware of the work of the DPBAC, despite the fact that we had taken evidence on the DA-Notice system in 2004, and reported on it in detail in our 2004–2005 Annual Report.*

[70] *Oral evidence – DPBAC, 20 January 2009.*

[71] *Oral evidence – DPBAC, 20 January 2009.*

89. The Committee's concerns about the current system centre around three main points. The first relates to the police. DA-Notice 5 (which relates to the intelligence and security Agencies) states that editors should seek advice from the DPBAC on information relating to:

> *Specific covert operations, sources and methods of the Security Service, SIS and GCHQ, Defence Intelligence Units, Special Forces and those involved with them, the application of those methods, including the interception of communications, and their targets; the same applies to those engaged on counter-terrorist operations.*

90. Sir Bill Jeffrey elaborated: *"It doesn't cover police operations, and ACPO [the Association of Chief Police Officers] has its own arrangements for talking to the media,"* and Mr Bucks was very clear that: "*The media would strongly resist any attempt to extend the existing system to cover… for example police matters."*[72]

91. The Committee considers, however, that this maintenance of the status quo fails to take into account the change in the world they are reporting on. Although this means that mainstream police investigations are likely to remain outside the scope of the DPBAC, it is increasingly common for the police and the Security Service to work closely together on, for example, counter-terrorist investigations that are extremely sensitive in national security terms. There is nothing to prevent the DPBAC machinery being engaged in such cases, although that did not happen in the case referred to in our earlier report. We have been told that the DPBAC is now considering whether there is more that can be done to raise awareness of this among the Agencies and the media.

M. Both parties would therefore benefit from a discussion as to how to refine the system with regard to the police.

92. The second concern relates to the informality of the procedures in place. There is no automatic process, as the Secretary explained:

> *It does rely, in the main, on journalists, or editors, or authors coming to me, or if I hear that something is going on then I can go out to them.*[73]

93. This rather haphazard consultation process places a burden unfairly on journalists to know when to consult and when not to consult, and this can only result in failures in the system. The Committee therefore considers that there should be a more formal process of consultation.

---

[72] *Oral evidence – DPBAC, 20 January 2009.*

[73] *Oral evidence – DPBAC, 20 January 2009*

94. Our final concern relates to the lack of any real power. As Sir Bill Jeffrey said:

> *This is a voluntary set of arrangements and… we meet… the responsible editors and other senior media people, but if in the end the journalist decides to ignore the advice and print something, there's nothing we can do about it.*[74]

This was illustrated in a recent case where *The Sunday Times* published information that clearly fell under the DA-Notice system, yet it failed to consult the Secretary before the event, and then failed to respond to concerns raised both on the Media Side of the DPBAC and by the Secretary. In other words, *The Sunday Times* completely ignored the system and any subsequent remonstrations without any consequences. Given this example, it is manifest that there is a problem with the current system and further thought must be given to how to address this.

N. The Committee recognises that the DPBAC has done, and continues to do, some good work in providing a means for the media and government sides to talk in confidence with a view to protecting information that may prove damaging to national security.

O. Nevertheless, the Committee considers that, as with any system, there is room for improvement and a need to evolve, to ensure that it remains fit for purpose and abreast of changes to the structures and organisations it deals with. We have seen how sensitive the media are when it comes to suggesting change in this area, but we must emphasise that change does not inevitably mean legislation or regulation and that there is room to build on what has gone before and create a more practical and useful system for all those who use it. We recommend that both sides should seriously consider how to move forward on the difficult issues raised here.

[74] *Oral evidence – DPBAC, 20 January 2009.*

STRATEGIC FRAMEWORK AND INTELLIGENCE MACHINERY

The Office for Security and Counter-Terrorism and CONTEST

95. The Committee reported in its 2007–2008 Annual Report on the establishment of the Office for Security and Counter-Terrorism (OSCT) in the Home Office, and we visited them this year. OSCT is responsible for the co-ordination of the Government's counter-terrorism strategy, CONTEST, and some aspects of its delivery.

96. Since its establishment in March 2007, OSCT has expanded beyond its original remit – it now also encompasses:

- interception modernisation;
- the possible use of intercept as evidence in criminal trials;[75]
- delivering the PROTECT strand of CONTEST; and
- responsibility for planning security arrangements for the 2012 Olympics.

This expansion has resulted in an increase in staff from 270 in 2007 to 320 permanent staff as at January 2009.[76]

97. We were told last year that OSCT had been tasked with "refreshing" CONTEST and that that work was due to be completed by the autumn of 2008. The revised strategy, *Pursue Prevent Protect Prepare: The United Kingdom's Strategy for Countering International Terrorism,* was finally published on 24 March 2009.[77] Announcing its publication in Parliament, the then Home Secretary said:

> *The threat remains and is always evolving. The strategy takes that into account, draws on what we have learnt about how to counter it, and reflects the increasing resources that we have… made available to keep Britain safe… In publishing it, our primary aim is to reassure the British public that we are doing all in our power to protect this country.*[78]

98. The strategy outlines the Government's approach to counter-terrorism over the next three years, based on a series of planning assumptions[79] including:

- that al-Qaeda will retain the capability to conduct significant terrorist attacks;
- that terrorists will gain access to a wider range of lethal technology and will continue to aspire to use chemical, biological, radiological and nuclear weapons;

---

[75] *Interception modernisation and the use of intercept as evidence are covered in paragraphs 166 to 182.*

[76] *This figure was provided to the Committee during our visit to OSCT in January 2009.*

[77] *Cm 7547.*

[78] *HC Deb 24 March 2009 vol 490 cc 169–170.*

[79] *Cm 7547, pages 47–48.*

- that the Government's ability to reach and persuade those who support violent extremism will be limited; and
- that the terrorist threat against the UK will continue to diversify, with "self-starting" terrorist organisations becoming more of a threat.

99. One of the key, and yet most difficult, strands in CONTEST is PREVENT: it is this strand (which aims to *"stop people becoming terrorists or supporting violent extremists"*) that is essential to the success of reducing the long-term terrorist threat to the UK. In recognition of this, the Government has dedicated significant resources to PREVENT – £140 million for 2008/09.

100. Given the importance of this work, and the considerable funding it is receiving, it is essential that clear and transparent targets are in place against which progress can be measured. Last year we were told that it was still too early to measure real success or outcomes of PREVENT. This year, we have been told that progress on PREVENT is now being measured using outcomes and indicators set within a new International Counter-Terrorism Public Service Agreement (PSA)[80] covering 2008 to 2011. The PREVENT PSA contains three key outcomes:

i. Resilience in domestic communities: An improvement in the extent to which domestic Muslim communities reject and condemn violent extremism.

ii. Resilience in sectors and services: A reduction in the risk of individuals who come into contact with key sectors/services [including prisons and higher education] becoming or remaining violent extremists.

iii. Resilience in overseas priority countries: A positive UK contribution to the resilience of priority countries to violent extremism.[81]

P. The PREVENT strand of CONTEST is crucial if we are to counter the long-term terrorist threat. While the results of this work may take time to be seen, it has now been two years and we would have hoped that progress could by now be evaluated against more quantifiable outcomes. We therefore recommend that more effective measures are developed against which to assess progress.

Research, Information and Communications Unit

101. One of the units within OSCT working under the PREVENT strand is the Research, Information and Communications Unit (RICU), which was established in June 2007 in order to counter extremist messages. It aims to:

- ensure consistency, across government, on counter-terrorism and counter-extremism messages;

---

[80] *Public Service Agreements (PSAs) are agreed by HM Treasury and departments as strategic performance measures. PSA 26 has been introduced for 2008–11, with the core aim of reducing the risk to the UK and its interests overseas from international terrorism.*

[81] *Letter from the Home Office – 17 March 2009.*

- provide a unified communications strategy across all departments involved in delivering aspects of PREVENT;
- undertake a wide range of "audience research" in order to identify how best to deliver these messages; and
- advise police forces and local authorities on how best to communicate with local communities in order to target those most at risk of turning to extremism.

In early 2009, RICU's remit was widened to include the co-ordination of PREVENT-related news across Whitehall, and responsibility for preparing communications strategies to underpin all four strands of CONTEST.

102. The Unit is jointly funded by the Home Office, the Foreign and Commonwealth Office (FCO) and Communities and Local Government, but is based in OSCT. RICU currently has 35 staff and a budget of £5.7 million for 2009/10. Of this budget, £1.5 million is expected to be spent on research, and £3.5 million on campaigns to *"empower community voices"* such as Muslim community groups.[82]

103. Given our concerns about the difficulty of measuring the success of work on PREVENT as a whole, we asked RICU how it was measuring its contribution. We were told that there were four key strands: *"measuring changes in audience attitudes; analysis of public discourse on counter-terrorism; stakeholder views; and evaluation of RICU campaigns and intervention"*. Asked about RICU's tangible successes so far, we were told that:

> *During the Gaza conflict RICU ensured that the Government's position was communicated… a major counter-narrative campaign has been initiated… a network of community organisations established… local partners in priority areas have been briefed and provided with communications advice… relationships have been built with key media channels… research into audience segmentation… has been completed… [and] guidance on communicating with Somali and Pakistani [communities] in the UK has been circulated.*[83]

104. RICU has now been in existence for over two years; however, the same concerns apply here as to the wider PREVENT strand (under which RICU falls): this is a difficult area of work where progress takes time, and is hard to see and measure. We hope that the results will be visible in the future, but note that RICU itself has said that *"communications can only take us so far"*.[84]

Security for the 2012 Olympics

105. As mentioned in paragraph 96, OSCT has expanded its remit to include Olympic and Paralympic security. The strategy for ensuring the security and safety of the Games is based on the Government's counter-terrorism strategy (CONTEST), and consists of five strands:

---

[82] *Letter from the Home Secretary – 13 May 2009.*

[83] *Letter from the Home Secretary – 13 May 2009.*

[84] Muslim Grievances – What They Are and Our Response, *RICU/16/07, 9 January 2007.*

- protect venues, events and infrastructure;
- prepare for possible disruption;
- identify and disrupt threats to the safety and security of the Games;
- command, control, plan and resource the safety and security operation; and
- engage with international and domestic partners, and communities, to enhance the security of the Games.

This is a major piece of work and we do not underestimate the effort that is going to have to be allocated to it in the run-up to 2012. We are, however, reassured by our initial discussions with the Agencies about the impact that it will have on them. The Director General of the Security Service, for example, explained that *"the overall counter-terrorism machine that the Government has been putting together over the last five years should be able to accommodate quite a lot of the work associated with the Olympics"*.[85] We will continue to examine plans as they progress, and assess whether sufficient resources are being devoted to this very considerable task.

The National Security Strategy

106. We reported last year on the publication of the Government's National Security Strategy.[86] We returned to it this year to find out what impact, if any, the new strategy has had on the work and priorities of the Agencies. The Agencies have reported to us that, as they expected, there has been little direct impact on the focus or nature of their work.

The National Security Forum

107. When the Prime Minister announced the National Security Strategy in March 2008, he also outlined plans for a National Security Forum[87] to advise the Ministerial Committee on National Security, International Relations and Development (NSID) on the strategy. The Cabinet Office told the Committee that it is envisaged that the Forum would meet around six times a year and described its expected composition:

> *It will be a mixture of specialists… we would look at a range of the different areas that are represented in the National Security Strategy… [these will] include the intelligence and security field, including diplomacy… the military, including the police, but also science, academia, interest in conflicts and international developments [and]… have one or two lay representatives as well.*[88]

108. However, we understand that the Forum will not now be appointed until 2010 and that, in the meantime, an interim forum has been appointed that, we were told on 8 April 2009, had met only once.[89] Progress appears to have been painfully slow, given the

---

[85] *Oral evidence – Security Service, 10 February 2009.*

[86] *The Government published an update to the National Security Strategy on 25 June 2009.*

[87] *The Cabinet Office has told us that the National Security Forum will take the form of a non-departmental public body.*

[88] *Oral evidence – Cabinet Office, 18 November 2008.*

[89] *Letter from the National Security Secretariat – 8 April 2009.*

importance the Government attaches to the National Security Strategy and its supporting structures.[90] Having said this, the impact of the National Security Strategy and Forum on the intelligence and security Agencies is very small, and these delays have not therefore had any bearing on their work. In addition, NSID and its sub-committees appear to have been functioning adequately without any significant advice from the Forum so far.

Q. The slow progress in establishing the National Security Forum appears to have had a negligible impact on the other elements of the national security machinery (including the strategy itself, the Agencies, and the Ministerial Committee on National Security, International Relations and Development). We therefore question whether the National Security Forum is in fact a necessary part of the National Security Strategy machinery.

The Joint Intelligence Organisation

The Joint Intelligence Committee

109. The Joint Intelligence Committee (JIC) is responsible for approving the UK's requirements and priorities (R&Ps) for secret intelligence collection. In April 2008, the JIC agreed to adopt a new approach to setting the R&Ps. The reason given was that, although demand for intelligence across a range of areas had grown, it was not being met due to the continued emphasis placed on a small number of priority requirements – in particular, international terrorism. In response, a new matrix approach was adopted, with secret intelligence collection priorities set on the basis of the strategic policy requirements contained in the National Security Strategy.

110. This new process for setting intelligence collection priorities marks a significant departure. We asked the Chair of the JIC what the long-term benefits are expected to be:

> *One of the benefits of the new way of doing things is that it provides effectively an audit trail so you can understand how you arrived at particular judgements… you have got weights assigned to the National Security Strategy objectives… The JIC was much more focused on the big picture and there was much less… nitpicking on individual issues.*[91]

111. The first set of R&Ps under this new system, covering the period 2009/10, was endorsed by Ministers in January 2009, with priority given to the following areas:

- counter-terrorism;
- supporting military operations – where HM Forces are on active service;
- weapons of mass destruction and counter-proliferation;
- countering state-led threats;
- maintaining military capability;

---

[90] *We also note that the Joint Committee on the National Security Strategy has yet to be appointed.*

[91] *Oral evidence – Joint Intelligence Organisation, 25 November 2008.*

- tackling trans-national organised crime;
- tackling global instability and conflict;
- promoting energy security;
- delivering economic wellbeing;
- developing strong and effective international institutions;
- avoiding dangerous climate change; and
- reducing international poverty and inequality.

In terms of country targets, the top priorities for 2009/10 are ***.[92]

112. We understand that the new system is also intended to provide greater flexibility to ensure more effective intelligence collection in response to unforeseen international events. The Director of GCHQ told us:

> *[The new process] allows us to deal more quickly when new requirements come to the fore. Trends are more visible, so concerns over *** sort of fall out of the new system more easily, and global and regional issues such as energy security and climate change are better highlighted… It does support a more dynamic treatment of priorities.*[93]

113. However, the Chief of SIS has informed us that, in effect, he sets his own priorities quite distinct from those established by the JIC:

> *The JIC priorities are not gospel as far as SIS is concerned. We do have to make our own judgement as to where we put our operational resource, and that is my responsibility under the statute. Nobody tells me I have to report to the JIC. I am responsible for the proper operational conduct of our business, so therefore it is my duty, and our duty, to make our own judgements about where we invest.*[94]

The relationship between the Agencies' priorities and the JIC priorities is an issue we intend to look into in greater detail next year.

Professional Head of Intelligence Analysis

114. One of the key changes arising from the Butler Review was the creation of the Professional Head of Intelligence Analysis (PHIA) role in order to provide a champion for analysts, and provide a career path for this group of specialists. We reported last year our concerns about the plan to subsume the PHIA role within the JIC Chair's post, since we considered that this would lessen the priority given to this crucial role.[95] In its response

---

[92] *The JIC told the Committee that, in addition to meeting requirements on these areas, it had also looked at the implications of the economic downturn. We were told that the JIC took the impact of the downturn into account "*on almost all the issues we look at*". (Oral evidence – Joint Intelligence Organisation, 25 November 2008.)*

[93] *Oral evidence – GCHQ, 24 February 2008.*

[94] *Oral evidence – SIS, 27 January 2009.*

[95] *Cm 7542.*

to our report, the Government said that the PHIA role was being subsumed into the JIC Chair's post in order *"to enhance its status and authority"*.[96] This change has now been implemented.

115. Alex Allan, the JIC Chair, has written to the Committee to reassure us that the change does not mean that the work of the PHIA is not being carried out. He said that he takes the role *"very seriously"*, although it appears that the day-to-day work is being carried out by a "Deputy PHIA", appointed in November 2008. Mr Allan told the Committee:

> *[The Deputy PHIA] is separate from the Assessments Staff, distant enough to be able to perform effectively in roles such as challenging assessments, but close enough to the assessment process to understand its intricacies. He attends JIC meetings as an advisor, and has direct access when needed to senior officials in the Intelligence Agencies and other departments. He takes on executive functions as well as day-to-day management of PHIA and reports directly to me.*[97]

This is nevertheless a deputy role, and in effect the work has therefore been downgraded.

R. The Committee does not accept the Government's response to our recommendation made last year, nor do we approve of the changes that have been made to the Professional Head of Intelligence Analysis (PHIA) role, which directly contradict our recommendations. We reiterate that the PHIA, established as a result of the Butler Inquiry, must have a distinct and separate role.

Challenge Team

116. In the past, the "Challenge Team" – whose role it is to question the veracity of JIC products – reported to the Head of the Assessments Staff, who is responsible for drafting those products. Recognising that this could be seen as "marking their own work", the reporting arrangements have been changed so that the team now reports to the Deputy PHIA. However, with that role now reporting directly to the JIC Chair (as PHIA), the team that has responsibility for scrutinising and challenging intelligence assessments now reports ultimately to the Chair of the body that oversees those assessments – in effect the same problem.

S. We welcome the fact that the "Challenge Team" in the Joint Intelligence Organisation has been moved from the Head of the Assessments Staff to the Deputy Professional Head of Intelligence Analysis (PHIA). However, as the PHIA post has now been subsumed within the JIC Chair, the team's independence has not, in reality, been increased. The JIC Chair is now performing the role of both "gamekeeper" and "poacher", undertaking a challenge function in relation to his own work. This reinforces our earlier view that the PHIA must be a separate and distinct role.

---

[96] *Cm 7543.*

[97] *Letter from JIC Chair – 22 June 2009.*

The Defence Intelligence Staff

117. During 2008/09, the Defence Intelligence Staff (DIS) has continued its wide-ranging work in support of UK military operations, including in Afghanistan and Iraq. The Chief of Defence Intelligence (CDI) told us that some important lessons have emerged from DIS's recent experience in supporting UK military operations. In particular, from both Iraq and Afghanistan:

> *The biggest lessons we have learnt in the intelligence world are the need to fuse intelligence from a range of different sources… to get the best possible picture that you can.*[98]

118. The Defence Human-sourced Intelligence (HUMINT) Unit is a critical part of DIS's intelligence collection assets in support of UK military operations. CDI told us that in both Iraq and Afghanistan the value of HUMINT *"has perhaps been much greater than we have seen in previous operations".*

119. We were therefore concerned to be told that:

> *[Although] Defence HUMINT assets continue to be heavily engaged in current operations with some notable successes… the ability of the Unit to support these operations and a range of additional commitments… remains fragile.*[99]

CDI told us that DIS has been committed to developing HUMINT capability in recent years, but that this was something that would take time:

> *Just like languages, HUMINT capability is not something we can grow overnight. To build up capability that you are prepared to use in what are, quite frankly, some very dangerous places takes time.*[100]

120. In addition to its core work in supporting military operations, other key areas of activity for DIS have included:

- contributing to the work of the joint US/UK Joint Narcotics Analysis Centre (JNAC), whose analytical products have helped develop a more informed approach to tackling the drugs trade in Afghanistan; and
- work to exploit foreign weapons systems, which has led to a number of significant benefits in both Iraq and Afghanistan.[101]

---

[98] *Oral evidence – DIS, 3 March 2009.*
[99] *Letter from DIS – 17 December 2008.*
[100] *Oral evidence – DIS, 3 March 2009.*
[101] *Letter from DIS – 17 December 2008.*

121. One of the key challenges for DIS is processing and analysing the considerable volume of intelligence collected. The Committee was told that this means that:

> *We need to prioritise ruthlessly, [and] we need to make absolutely clear that our customers understand that we can't deal with everything that is collected, and... they need to be absolutely clear what question it is that they want answered… a question such as "tell me everything you know about" is not good enough for a modern intelligence system.*[102]

122. Having been told that there are insufficient resources to meet the requirements of DIS customers, the Committee has further investigated the staff cuts about which we expressed concern last year.[103] We have now been told that there will be a reduction of 122 posts, of which just under half are analytical staff.[104] DIS informed us that the impact of these staff losses was being mitigated by moving all London staff into a single open-plan Whitehall location, improving IT systems, and internal restructuring.[105] However, CDI conceded that, despite these changes, cuts will nevertheless mean that:

> *In some areas we are still covering the area but with perhaps fewer people and in other areas we have had to drop outputs completely… those are the outputs that we have assessed with a broad consultation to be the lowest priorities for us, but obviously for our customers, most importantly…it will be a question of trying to maintain our output with a smaller number of people and maintaining the flexibility in order to do that.*[106]

T. The Committee remains concerned that these reductions in Defence Intelligence Staff (DIS) staff numbers will have a serious impact on DIS capability. They could also have long-term implications for DIS core customers and the wider intelligence community.

SCOPE

123. The SCOPE programme was established in 2001 as a major interdepartmental IT project designed to facilitate more efficient and effective information sharing across the wider intelligence community. It was intended to be delivered in two phases:

- Phase 1: connecting key departments (such as the Home Office and SOCA) to the existing secure communications network used by the intelligence community; and
- Phase 2: improving and expanding the secure communications network and extending the system's capabilities.

---

[102] *Oral evidence – DIS, 3 March 2009.*

[103] *Cm 7542.*

[104] *Letter from DIS – 17 December 2008.*

[105] *In January 2009, DIS reviewed its internal structures and created three main divisions, with the aim of still being able to meet customer demands but with fewer analytical staff. It has also reviewed and reorganised its internal structure, and has created three new divisions: a reformed strategic assessment division; a capability assessments division; and a new counter-proliferation division.*

[106] *Oral evidence – DIS, 3 March 2009.*

124. SCOPE has been dogged continually by problems and we have repeatedly voiced concerns about the programme. After a two-year delay, Phase 1 was eventually implemented in late 2007, and the Committee was assured (in January 2008) that concerted efforts were being made to ensure successful and timely delivery of Phase 2. However, just three months later, as we reported last year, the decision had been taken to abandon SCOPE Phase 2. We reported that we were appalled at what appeared to be a waste of tens of millions of pounds, and said that we would be investigating why this vital project failed, the associated cost implications and the options for a replacement system.[107]

U. We had hoped to include in this Report a detailed account of the Cabinet Office's decision to abandon Phase 2 of the SCOPE programme. However, the Committee is still investigating the circumstances surrounding the decision, and commercial and legal negotiations between the Cabinet Office and contractor continue. We will therefore report on this matter in our next report.

CLiC

125. Following the failure of SCOPE Phase 2, GCHQ and SIS set up an initiative called Collaboration in the Intelligence Community (CLiC). This is intended to be a low-risk, inexpensive approach, providing incremental changes to existing systems, and designed to address the intelligence community's most urgent IT collaboration requirements. The Chief of SIS told us:

> *CLiC is designed to shore up... some of the capability that SCOPE 2 would have given us... We are doing really quite well on this more modest CLiC programme, which is not being run out of the Cabinet Office, it is being run out of SIS and GCHQ... and it will be of community-wide value when it is delivered.*[108]

126. The first three areas CLiC will address are:

- development for Her Majesty's Revenue and Customs (HMRC) of an enhanced version of the SCOPE Phase 1 Top Secret desktop, which will enable HMRC to continue to receive intelligence and communicate securely via email. This approach will reduce the overall cost of Top Secret desktop systems through economies of scale;
- STRAP3A secure messaging – an email system for intelligence information that is subject to the highest protection standards. It is planned that, by the end of the 2009/10 financial year, up to seven departments (GCHQ, SIS, Ministry of Defence, FCO, Security Service, Cabinet Office and Home Office) will be able to exchange information at this level; and

[107] *Cm 7542.*
[108] *Oral evidence – SIS, 27 January 2009.*

- a pilot programme for 100 users to collaborate on serious crime work. GCHQ has told us that this pilot successfully delivered, over a two-month period, the UK's first Top Secret "shared workspace" between GCHQ, SIS and SOCA. In May 2009, we were informed that the next planned increment will be the expansion of the user base to around 600 to 700 users across the wider intelligence community.

127. A total of £*** million was spent on CLiC between August 2008 and the end of March 2009, with SIS and GCHQ each contributing £*** million and the remaining sum being provided by HMRC and the FCO. The largest cost element has been for specialist contractor staff and the development of technical infrastructure, with ***.

V. CLiC appears to be progressing well so far. We are optimistic that it will deliver some of the IT solutions that the (far more costly) SCOPE Phase 2 programme was unable to. It is regrettable that this same practical and incremental approach was not adopted in the planning of the SCOPE programme.

SCOPE Overseas

128. The SCOPE Overseas project was initiated in November 2005, with the aim of providing secure email between some overseas posts and other domestic users on the UK Intelligence Messaging Network (UKIMN).

129. The UK infrastructure for SCOPE Overseas became operational in mid-2008. There are now 12 posts connected to the UKIMN: ***
***.
In May 2009 the FCO told the Committee that *** would be connected in the coming months. The system will be rolled out to around 40 posts by March 2010. There is currently no FCO funding for further installations beyond April 2010.

The Commissioners

130. The Intelligence Services Commissioner has responsibility to keep under review the issue of warrants by the Secretary of State authorising intrusive surveillance and interference with property in order to make sure that the Secretary of State has the right to issue them.[109] His responsibilities include reviewing the Agencies' authorised use of directed and intrusive surveillance (the covert monitoring of targets' movements, conversations and other activities) and of covert human intelligence sources, to check that the Agencies are acting in accordance with the law.

131. The Interception of Communications Commissioner has responsibility to keep under review the issue of interception warrants and the adequacy of the arrangements for ensuring that the use of product of interception is properly handled.[110]

---

[109] Report of the Intelligence Services Commissioner for 2007, *HC948.*

[110] Report of the Interception of Communications Commissioner for 2007, *HC947.*

132. Both Commissioners' roles are central to maintaining public trust that the Agencies operate within the law in relation to their use of both intercepted communications and surveillance.

133. The Committee held informal discussions with both Commissioners during the year to discuss areas of common interest. Both reported that, while there had been a significant increase in applications for the issue of warrants, this had not been particularly notable in light of the current security environment and increased counter-terrorism work. Overall, they were impressed by the Agencies' performance in this field and their improved audit trails.

134. In addition to their statutory responsibilities in the reviewing of warrant applications, the Commissioners told the Committee that they are also currently engaged in other key projects:

- The Interception of Communications Commissioner, Sir Paul Kennedy, reported that he had been asked to assist in the preparations for the "judicial role-play" component of the Intercept as Evidence (IaE) Implementation Project.[111]
- The Intelligence Services Commissioner, Sir Peter Gibson, told the Committee that he had been asked by the Prime Minister to provide him with a personal assurance that the Agencies had conducted sufficiently rigorous searches of their records with respect to allegations of complicity in the torture of detainees.

[111] *Intercept as evidence is discussed in paragraphs 166 to 178.*

OTHER ISSUES

Diego Garcia

Background

135. In July 2007, the Committee published its report into rendition,[112] which considered:

> *Whether the UK intelligence and security Agencies had any knowledge of, and/or involvement in, rendition operations (including specific cases), and their overall policy for intelligence sharing with foreign liaison services (principally the United States) in this context.*[113]

136. Although the focus of our rendition inquiry was on the actions of the UK Agencies, we also, as necessary background, looked at allegations that US rendition operations had transited UK territory or airspace (including that of Overseas Territories). One matter that we considered was whether any rendition flights had transited Diego Garcia (in particular, in September 2002).

Committee findings

137. We asked the then Prime Minister about this allegation and reported his response, in March 2007, that the US had given firm assurances that no detainees had transited through the territorial seas or airspace surrounding Diego Garcia.

Information that has come to light since our report was published

138. On 20 February 2008, however, the Foreign Secretary informed the Committee that a recent US investigation of its records on rendition flights had discovered that there had in fact been two rendition flights through Diego Garcia in 2002.[114] He made a statement to the House the following day, saying:

> *The US Government have assured us that no US detainees have ever been held on Diego Garcia... the US Government have told us that neither of the men [on board those flights] was a British national or a British resident. One is currently in Guantánamo Bay. The other has been released.*[115]

---

[112] *Cm 7171.*

[113] *"Rendition" encompasses any extra-judicial transfer of persons from one jurisdiction or state to another. "Extraordinary rendition" is usually used to refer to a rendition for the purposes of detention and interrogation outside the normal legal system, where there is a real risk of torture or cruel, inhuman or degrading treatment. A full explanation is included in the Committee's report into rendition (Cm 7171) on page 6.*

[114] *The then Director of the Central Intelligence Agency (CIA), Michael Hayden, also made a statement on 21 February 2008 that made it clear that the CIA did not operate a holding facility on Diego Garcia. The US also said that neither individual was held as part of the CIA's high-value target interrogation programme.*

[115] *HC Deb 21 February 2008 vol 472 cc 547–548.*

139. The Foreign Secretary subsequently told the Committee:

> *On both occasions, in January and September 2002, the prisoner remained on board and was then flown to a further location. We have been informed that the aircraft were on the ground in Diego Garcia for 1 hour 40 minutes and 2 hours 30 minutes respectively.*[116]

140. As a result of this new information from the US, the Foreign Office compiled a list of flights where the FCO had been alerted to concern about rendition through the UK or the Overseas Territories, and asked the US to perform rigorous checks to confirm that there were no additional cases. The Foreign Secretary told Parliament on 3 July 2008:

> *The United States Government confirmed that, with the exception of two cases related to Diego Garcia in 2002, there have been no other instances in which US intelligence flights landed in the United Kingdom, or Overseas Territories, or the Crown Dependencies, with a detainee on board since 11 September 2001.*[117]

141. The Committee asked the Foreign Secretary for further details as to what records were held on these two flights. The Foreign Secretary told the Committee (in July 2008) that records on flights landing in Diego Garcia in 2002 would have been held for no longer than five years.[118] The Foreign Secretary told the Committee:

> *These flights would have been recorded in the General Declaration made by the aircraft and also in the Customs and Immigration Daily Occurrence Log. These are generally held for 3 and 5 years... respectively. In addition, the British representative on Diego Garcia... is provided with a rolling flight schedule by the US at least daily which has the following week's flights detailed. This is used for short-term administration and it is not retained for record-keeping purposes. In view of the points set out above, records are unfortunately no longer held for the period when the two cases of rendition occurred.*[119]

It appears, therefore, that there is no guarantee that the information uncovered to date is in fact complete. This situation is clearly unsatisfactory, although we note that the FCO has now instructed all Overseas Territories to maintain all flight records until further notice, and that this should ensure that a similar situation does not arise again.

142. While these problems – caused by a lack of adequate records – are a matter for concern, what is more significant is what the incidents reveal about the relationship between the UK and the US. The agreement signed in 1980 between the US and UK governing the shared use of Diego Garcia[120] states that "*... the [United States Government] will continue the practice of consulting HMG [Her Majesty's Government] prior to any politically sensitive use of Diego Garcia*". The onus was therefore on the US to notify

---

[116] *Letter from the Foreign Secretary – 13 March 2008.*

[117] *HC Deb 3 July 2008 vol 478 cc 58ws.*

[118] *Letter from the Foreign Secretary – 31 July 2008.*

[119] *Letter from the Foreign Secretary – 31 July 2008.*

[120] *Memorandum of Conversation dated 13 June 1980, interpreting the provisions of a 1976 US–UK treaty concerning Diego Garcia.*

the UK, and it would appear that this did not happen on these occasions. The Foreign Secretary has since sought fresh assurances from the United States:

> *Our US allies are agreed on the need to seek our permission for any further renditions through UK territory... We have made clear that we would only grant such permissions if we were satisfied that the rendition would accord with UK law and our international obligations.*[121]

W. While the then Prime Minister's specific assurances to this Committee, in relation to Diego Garcia, were on the basis of firm assurances from the United States, these recent developments have demonstrated that the UK must be more robust in verifying such assurances in the future.

Individual allegations of UK involvement in or knowledge of torture by foreign liaison services

143. During our investigations into rendition[122] and *The Handling of Detainees by UK Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq,*[123] the Committee considered the policies of the UK intelligence and security Agencies in relation to torture or cruel, inhuman or degrading treatment (CIDT). Our report on rendition summarised the position as follows:

> *The Security and Intelligence Agencies do not participate in, solicit, encourage or condone the use of torture or inhuman or degrading treatment. For reasons both ethical and legal, their policy is not to carry out any action which they know would result in torture or inhuman or degrading treatment.*[124]

144. During the House of Commons debate on the Committee's 2006–2007 Annual Report,[125] which took place on 17 July 2008, the then Home Secretary reiterated this policy when she said: *"This country and its intelligence and security Agencies abhor torture and neither condone nor support the ability of others to carry it out."*[126]

145. There have been, since our inquiry into rendition, a number of allegations that, contrary to established policy, the UK intelligence and security Agencies have been involved in the mistreatment of certain individuals detained by foreign governments. Individual complaints regarding the conduct of the UK Agencies are a matter for the Investigatory Powers Tribunal to investigate and, therefore, any such cases should be referred to them.[127] Nevertheless, this Committee considered that some of the allegations

---

[121] *HC Deb 3 July 2008 vol 478 cc 58ws.*

[122] *Cm 7171.*

[123] *Cm 6469.*

[124] *Cm 7171, paragraph 174.*

[125] *Cm 7299.*

[126] *HC Deb 17 July 2008 vol 479 c458.*

[127] *The Investigatory Powers Tribunal is a body of senior figures from the legal profession, under a president who is a senior member of the judiciary, which was established under the Regulation of Investigatory Powers Act 2000. The Tribunal can investigate allegations of unwarranted or disproportionate action by the Agencies, or alleged breaches of human rights. The Tribunal can be contacted by writing to The Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ, by telephoning 020 7035 3711, or via www.ipt-uk.com.*

– particularly in relation to Mr Mohamed – gave rise to policy questions that needed to be investigated.

Binyam Mohamed al-Habashi

Background

146. During the Committee's inquiry into rendition, one of the specific cases we considered was that of Mr Mohamed and the allegation that UK Agencies were either complicit in, or aware of, both his rendition and the alleged torture that followed.[128] Mr Mohamed has alleged that while detained in Pakistan he was abused by the Pakistanis, and that during his detention he was interrogated by American and British officials.[129] He claims that he was sent to Morocco, where he was tortured, and that information used by his interrogators had been provided by the UK Government.

Initial findings

147. Our investigation confirmed that, while detained in Karachi, Mr Mohamed[130] had been interviewed for approximately three hours by a mid-ranking officer from the UK Security Service. The Security Service denied that the officer told him he would be tortured. The Service also told the Committee that no signs of abuse were evident during the interview and no allegations of abuse were made. However, during our original inquiry, the Director General of the Security Service (Dame Eliza Manningham-Buller at that time) did say that MI5's involvement in this case was one *"... where, with hindsight, we would regret not seeking proper full assurances at the time"*.[131]

Events subsequent to publication of our report into rendition

148. On 28 May 2008, Mr Mohamed was charged with terrorist offences under the US Military Commissions Act. Evidence against him included confessions he made during detention in Bagram, Afghanistan between May and September 2004, and at Guantánamo Bay prior to November 2004. He contended that this evidence was inadmissible because it was obtained when he was being held incommunicado and subject to torture and cruel, inhuman or degrading treatment (CIDT) at the hands of the Pakistani and Moroccan authorities, assisted by the US Government.

149. In support of his case at Guantánamo, his lawyers sought an order against the Foreign Secretary for the disclosure of information in confidence to his lawyers on the basis that it may support his argument that his confessions were obtained by torture or CIDT. In parallel, through his habeas corpus case in the US District Court, his US lawyers pursued the release, by the US authorities, of US-sourced material that his defence team believed to be exculpatory.[132]

---

[128] *Mr Mohamed was arrested in Pakistan in April 2002 and was subsequently detained by US authorities in Guantánamo Bay, Cuba. He was released from custody and returned to the UK in February 2009.*

[129] *Reprieve written submission to the Committee, 4 December 2006.*

[130] *Mr Mohamed has been referred to by a number of other aliases.*

[131] *Cm 7171, paragraph 105.*

[132] *Mr Mohamed's habeas corpus case was launched in April 2005 to challenge the basis of his detention in Guantánamo Bay, following a Supreme Court ruling, in July 2004, that the US courts had such jurisdiction. Although all habeas corpus cases were quashed by the 2006 Military Commissions Act (MCA), this was overturned by the Supreme Court ruling of 12 June 2008 in Boumediene v. Bush, which ruled the MCA unconstitutional and reinstated habeas corpus rights.*

150. In May 2008, the Security Service wrote to the Committee informing us that, in the course of reviewing its records in preparation for the judicial review of the Foreign Secretary's decision not to release papers to Mr Mohamed's lawyers, it had discovered information that had not been shared with the Committee during our rendition inquiry. The Security Service first wrote on 22 May and then again, with further information, on 30 June 2008, and SIS wrote on 14 August and 2 October 2008.

151. Their letters informed the Committee that information from US liaison, containing details of the US interrogation of Mr Mohamed, had been provided to the Security Service and SIS in May 2002, before the Security Service officer interviewed Mr Mohamed. This information made it clear that Mr Mohamed had been intentionally deprived of sleep by his captors while in detention in Pakistan. For example, one of the *** telegrams states:

> ***
> ***
> ***.[133]

152. The Security Service officer who interviewed Mr Mohamed on 17 May 2002 said that he could not recall whether or not he was aware of this information prior to the interview. There is no record that the Security Service took any action on receipt of this information: it continued to provide US liaison with background information, and questions to be put to Mr Mohamed, up until April 2003. (There is no record of the UK passing further information regarding Mr Mohamed to the US after this date.[134])

153. The High Court delivered its first judgment on Mr Mohamed's case on 21 August 2008. A further two judgments were issued on 29 August and 22 October, following developments in the US. Lord Justice Thomas and Mr Justice Lloyd Jones concluded that the case in the High Court should be postponed until the related legal proceedings in the US had concluded. In October 2008, after pressure from the UK Government, the US authorities agreed to an exceptional disclosure of all the documents at issue in the judicial review to Mr Mohamed's US lawyers through his habeas corpus case in the US. On 21 October 2008, the Convening Authority dismissed, without prejudice, all the charges against Mr Mohamed. This followed the resignation of the prosecutor in Mr Mohamed's case. The prosecutor had separately expressed concerns in public that evidence was being suppressed in an unrelated case.

154. With Mr Mohamed's lawyers in possession of the documents at issue, the US charges against him dropped, and his release from Guantánamo Bay in February 2009, the focus of the case in the High Court shifted away from seeking justice for Mr Mohamed. The new focus of the case was to determine whether the public interest in publishing a summary of US intelligence material relating to Mr Mohamed's treatment in Pakistan was outweighed by the potential damage to national security arising from the publication of classified US intelligence material.

---

[133] *Telegram from *** entitled "***" sent to the Security Service and SIS on 15 May 2002.*

[134] *However, information relating to Mr Mohamed continued to be received from the US into 2004.*

155. On 4 February 2009, the High Court issued its fourth judgment in this case. The judges accepted the Foreign Secretary's assessment that the release of classified US material into the public domain by a UK court would damage the UK's intelligence relationship with the US. However, following comments made by the Foreign Secretary in the House of Commons,[135] that the US had not threatened to "break off" intelligence co-operation with the UK, Mr Mohamed's lawyers applied to the court to reopen its fourth judgment on the grounds that it had been misled regarding the existence of a "threat" and as to the position of the Obama administration. This Report covers the period up to July 2009 and therefore subsequent developments in this case have not been covered here. The Committee will comment on these in its next Annual Report.

Further investigation

156. While this Committee does not investigate individual cases, as these are properly a matter for the Investigatory Powers Tribunal, we nevertheless considered that some of the issues raised by the case, and the allegations arising from it, were so serious that they went right to the heart of how our intelligence and security Agencies operate, the policies they implement and the procedures they follow. It is this aspect that is within our remit, and which we have been considering since we received the letter from the Director General of the Security Service in May 2008. We took evidence from the Heads of SIS and the Security Service, and from the Foreign and Home Secretaries, and considered the closed evidence submitted to the High Court as part of Mr Mohamed's case. We remain concerned that there may be implications for the intelligence-sharing relationship.

157. We wrote to the Prime Minister on 17 March 2009 regarding the policy implications of allegations that the UK was complicit in the mistreatment of detainees held overseas, in particular those arising from the case of Mr Mohamed. Due to a current police investigation into the actions of the Security Service officer who interviewed him in Pakistan on 17 May 2002, we cannot comment further publicly at this time.

Guidance on the treatment and interview of detainees

158. On 18 March 2009, the Prime Minister wrote to the Chairman inviting the Committee *"to review the current UK intelligence and security Agencies' guidance to their personnel concerning the treatment and interview of detainees to make certain that it is sufficiently clear to ensure that they act in accordance with UK and international law"*.[136] The individual sets of guidance were first to be consolidated into a single document by the Cabinet Office. At the time of writing we have not yet received this material from the Cabinet Office and have therefore been unable to begin our review.[137]

Record keeping

159. One of the issues arising from the Mr Mohamed case is the fact that relevant documentation was overlooked. The Security Service failed to discover all the relevant information when searching its records for this Committee's rendition inquiry (in 2007). Further relevant documents were discovered during searches of its records for

[135] *HC Deb 5 February 2009 vol 487 c990.*

[136] *Letter from the Prime Minister – 18 March 2009.*

[137] *The consolidated guidance was received on 18 November 2009.*

Mr Mohamed's case in the High Court (in 2008). During 2009, a further 20 documents relevant to Mr Mohamed's case were discovered, two of which were identified as a result of this Committee's questioning of the Agencies (which, in turn, prompted a further review, which led to the disclosure of an additional seven documents).[138]

160. In relation to the original oversight during our rendition inquiry, the Director General of the Security Service has told us:

> *The information in question should have been found when we... carried out wide-ranging searches of records at the time of the Committee's inquiry into rendition... I cannot fully explain why it was not discovered in... our... records... Service systems in place at the time should have located this information.*[139]

161. As regards SIS, it has told us that, despite the fact that it also held some of these records, it did not provide them to the Committee during our original inquiry because the search it conducted was limited in scope:

> *The information did not come to light when SIS trawled its records in connection with the Committee's rendition inquiry because of the search parameters used.*[140]

When we specifically asked SIS about the information, we were initially told that there was no indication that it had been passed to senior staff or to SIS officers stationed ***.[141] We asked SIS to check its records again and were subsequently told that at least four members of staff saw the information, including the team leader covering ***, and their section head.[142]

X. We regret that neither the Security Service nor the Secret Intelligence Service identified the relevant documentation in response to Committee requests or in support of evidence given to us by their respective Heads during our original rendition inquiry. There is no convincing explanation as to why this information was not made available to this Committee. While we do not believe that this was a deliberate attempt to deceive us, it highlights fundamental problems with the record-keeping systems and processes of both Agencies.

---

[138] *In April 2009, the Security Service provided the High Court with a total of 13 further documents relevant to Mr Mohamed's case that should have been disclosed previously. The first tranche, of nine documents provided on 9 April, consisted of documents that had not been reviewed for disclosure purposes owing to a misunderstanding between the Service and its counsel. Two of these documents had been identified as a result of questions provided to the Service by this Committee; their discovery prompted a further review by counsel, leading to the disclosure of the additional seven documents. The second tranche, of four documents provided on 17 April, were identified either as a result of a new search possibility that only came to light due to counsel's advice regarding disclosure of the first tranche or through electronic searches using additional spelling variants. A further four documents, discovered in electronic libraries that had only recently become word-searchable, were disclosed on 21 May. Finally, on 14 July, three other documents were disclosed, discovered through word searches of additional electronic libraries that had recently come to the attention of Security Service lawyers and were identified as potentially containing relevant information. The Committee has seen the full, classified versions of all these 20 newly disclosed documents. While we cannot report the contents of these documents, these recent developments have served to reinforce our concerns about record keeping in the Agencies.*

[139] *Letter from the Security Service – 30 June 2008.*

[140] *Letter from the Secret Intelligence Service – 14 August 2008. (The Committee has since been told that, in the future, the search parameters used will be shared with the Committee, along with the results of the search.)*

[141] *Letter from the Secret Intelligence Service – 14 August 2008.*

[142] *Letter from the Secret Intelligence Service – 2 October 2008.*

162. The Director General of the Security Service has assured the Committee that, after 9/11, the Service realised that the volume and pace of counter-terrorism work had begun placing pressure on its record-keeping systems. As a result, the Service made improvements to these systems with the aim of improving its ability to retrieve information. The Service's longer-term strategic investment in this area will, however, only be fully realised in 2011, and, for resource reasons, old records will not be transferred onto the new system. The Director General explained that:

> *We are [still] liable to find retrospectively documents that should have come to light earlier... I am unable to give you a categorical assurance... that this sort of problem could not occur again.*[143]

163. We have also been told that improvements to records management has been, and continues to be, a priority for SIS:

> *There is certainly an issue about the resource that we devote to this, but certainly, ever since I have been in this job, records management has been a big issue and... a major red risk... We have made a lot of progress on it and that progress reflects years of investment and training, not just a sudden knee-jerk reaction to the Binyam [Mohamed] issue.*[144]

Y. While we understand that the balance of the Agencies' effort must be focused on operational work, at the same time good record keeping is crucial. The Agencies' operational work is about knowledge and information, and the ability to retrieve such information is central to the work with which they are charged. We welcome the assurances we have received from the Security Service and the Secret Intelligence Service that they are taking action to rectify the problems with their records, although we note that it will take several years before new systems are fully established. This has serious ramifications – both in terms of the Agencies' own work and for the reliability of the evidence they submit to this Committee.

164. We have seen before how the issue of poor record keeping extends beyond the Agencies to their parent departments. During our inquiry into rendition, the Foreign and Commonwealth Office was unable to respond adequately to allegations of UK knowledge of, or involvement in, US rendition flights[145] and, since then, the FCO has told us that records on flights transiting Diego Garcia were only kept for three or five years and are therefore no longer available. In addition, during our *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005,* the Home Office was unable to provide the Committee with figures relating to the conviction of terrorists.

---

[143] *Letter from the Security Service – 30 June 2008.*

[144] *Oral evidence – SIS, 29 January 2009.*

[145] *The Foreign Secretary has told the Committee that the FCO has now taken action, taking a clear lead on rendition policy, improving its system of record keeping, and establishing points of contact across relevant government departments:* "The Departments are aware that if a request for assistance with a potential rendition operation is received it must be forwarded to the designated point of contact in the FCO. Similarly we have instructed our Overseas Posts to report to the FCO any request for assistance. This includes any over-flight requests which may have – or could be perceived to have – a rendition angle." *(Letter from the Foreign Secretary – 12 May 2008.)*

165. We have seen some improvement in departments' record-keeping systems and processes and therefore hope that we will not experience such problems in the future.

Intercept as evidence

166. The issue of whether intercept as evidence (IaE) should be admissible in criminal proceedings continues to be highly contentious.[146] Some commentators have long argued that the ability to adduce intercept material in criminal proceedings would significantly improve the ability to charge and prosecute terrorist suspects successfully.

167. In July 2007, the Prime Minister established a Privy Council Review led by the Rt. Hon. Sir John Chilcot to consider *"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"*.[147] The Chilcot Review was published in February 2008. It concluded that, in principle, intercept material should be admissible as evidence, subject to nine key operational requirements being met. These were reported in full in our 2007–2008 Annual Report.[148] The Government accepted the Review's recommendations and set up an Implementation Team, based in the Home Office, to explore the feasibility and practicalities of possible solutions. An Advisory Group of Privy Counsellors (AGPC) was established to advise the Implementation Team.[149]

168. On 9 February 2009, the AGPC produced an interim progress report on the first of the three phases of implementation work – "designing" a model for the use of IaE.[150] The report concluded that the work should now move on to Phases 2 and 3 ("model build" and "model test"). It recommended that the work should focus on the key issues underpinning operational and legal requirements, drawing out the likely impacts in practice on the operations of the intercepting Agencies, and on counter-terrorism and serious organised crime trials.

169. Nevertheless, the AGPC reported concerns about a number of outstanding issues, particularly the intrinsic tension between legal and operational requirements. As a result, the AGPC concluded that *"it would be wrong not to sound a clear note of caution"*[151] because:

> *Securing the intended increase in successful prosecutions while ensuring fairness of trial remains difficult and may not prove possible in most complex cases.*[152]

---

[146] *The Privy Council Review that reported in January 2009 was the seventh major review of IaE since 1995.*

[147] Privy Council Review of Intercept as Evidence*, Cm 7324.*

[148] *Cm 7542.*

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

[150] Intercept as Evidence – First Interim Progress Report of the Advisory Group of Privy Counsellors, *9 February 2009.*

[151] Intercept as Evidence – First Interim Progress Report of the Advisory Group of Privy Counsellors, *9 February 2009, covering letter.*

[152] Intercept as Evidence – First Interim Progress Report of the Advisory Group of Privy Counsellors, *9 February 2009, paragraph 11.*

170. We remain unconvinced as to whether IaE would make a difference. The then Home Secretary also told us:

> *I have asked, with respect to the ***, whether or not there would have been a different result in terms of the point at which people were released from pre-charge detention if intercept as evidence had been used, and there categorically the suggestion is that no, it would not have made a difference.*[153]

We were also told that in *** the use of intercept material would not have *"made a fundamental difference"*.[154]

171. The Committee has been briefed by the IaE Implementation Team. We have been impressed by the effort that all departments and Agencies are contributing to this project in the hope that it will provide a definitive answer to what has been a contentious issue.

Coroners and Justice Bill

172. A further issue related to the use of intercept material, which we referred to in our last Annual Report, was the proposal that intercept material should be disclosed in certain coroners' proceedings.[155] This was originally contained in the draft Counter-Terrorism Bill 2008 but was removed in October 2008. It subsequently reappeared as part of the Coroners and Justice Bill 2009.[156]

173. The Committee has previously indicated its concern that the provision of intercept evidence for the purposes of a coroner's inquest should have the same degree of protection as that outlined in the nine Chilcot tests. The AGPC shares our concern, recommending in its February 2009 report that:

> *Proposals for closed hearings in the present Coroners and Justice Bill should demonstrably secure the same or equivalent safeguards for use of intercept material as those set out in the Privy Council Review.*[157]

174. In order to address this issue, the Bill contained provision to enable the Secretary of State to certify an investigation if it would involve sensitive issues, including national security, diplomatic relations and serious crime. Certification in this respect means that the investigation would be conducted by a judge of the High Court. Where interception material is deemed by the judge to be relevant to the investigation, the inquest would be held without a jury.[158]

---

[153] *Oral evidence – Home Secretary, 28 April 2009.*

[154] *Oral evidence – Home Secretary, 28 April 2009.*

[155] *Cm 7542.*

[156] *Coroners and Justice Bill 2009 (Committee Stage), Part 1, Chapter 1, Section 12 – intercept evidence.*

[157] Intercept as Evidence – First Interim Progress Report of the Advisory Group of Privy Counsellors, *9 February 2009, covering letter.*

[158] *Draft Coroners and Justice Bill 2009, Part 1, Chapter 1, Section 11 – Certified investigations: investigation by judge, inquest without jury.*

175. The then Home Secretary had assured the Committee that the proposed exemption to section 18(7) of the Regulation of Investigatory Powers Act 2000 to permit disclosure of intercept material to the judge and counsel to the inquest would:

> *Not permit the disclosure of intercept material beyond the High Court judge conducting the certified investigation and counsel to the inquest. This process is designed to "maintain the ring of secrecy" just as the nine [Chilcot] operational tests are intended to do more generally.*[159]

176. The Government believed that the inclusion of sections 11 and 12 had:

> *Struck a fair and proportionate balance between the interests of bereaved families, the need to protect sensitive material and judicial oversight of the whole process.*[160]

However, during the progress of the Bill it became clear that:

> *The provisions still do not command the necessary cross-party support and in these circumstances the Government will table amendments to remove clauses 11 and 12.*[161]

177. While the Committee is pleased to see that clauses 11 and 12 have now been removed from the Bill, we note that the then Home Secretary told the Committee that:

> *This is a very difficult area where we need to reconcile the legitimate requirements of both security and transparency. In particular, the need to ensure such inquests are compliant with Article 2 of the ECHR*[162] *means that there is no "do nothing" option.*[163]

178. We have been told that, in order to resolve this problem, the Government is planning to use the Inquiries Act 2005, which already permits the use of intercept material, in those rare cases where intercept material is critical to the case: *"[The Government] will consider establishing an inquiry under the Inquiries Act 2005 to ascertain the circumstances the deceased came by his or her death."*[164] We have yet to be informed how this might work in practice.

---

[159] *Letter from the Home Secretary – 11 May 2009.*

[160] *Written statement by the Secretary of State for Justice and Lord Chancellor – 15 May 2009.*

[161] *Written statement by the Secretary of State for Justice and Lord Chancellor – 15 May 2009.*

[162] *Article 2 of the European Convention on Human Rights 1950 states that: "Everyone's right to life shall be protected by law." This has been interpreted by the European Court of Human Rights as including a duty to investigate all aspects of any suspicious deaths.*

[163] *Letter from the Home Secretary – 11 May 2009.*

[164] *Written statement by the Secretary of State for Justice and Lord Chancellor – 15 May 2009.*

Interception Modernisation Programme

179. Last year we reported that the Home Office had established the cross-government Interception Modernisation Programme[165] with a view to updating the way in which intelligence and law enforcement agencies collect and access lawful intercept and communications data. The aim of the work is to maintain current capability – not expand it – in the face of the *"most significant communications changes since the development of the telephone".*[166]

180. The programme is primarily focused on the collection of technical details about a communication, and not its contents. Communications data is critical in enabling investigators to identify suspects, provide key evidence and support the lawful interception of communications. (We have been informed that communications data has played a significant role in all Security Service investigations since 2004.[167])

181. The then Home Secretary informed the Committee that the cost of the programme was in the region of £300 million and that the estimated ten-year costs of the programme were *"at the high end of £2 billion"*. We were also told that:

> *This is not just money well spent but money absolutely crucially spent if you want to maintain the ability of law enforcement and the Security Service and others to do the job... not an improved job, but the job we expect them to do now. Because what we are faced with is a potential degrading of the capability as technological developments and market developments happen in the communication market.*[168]

182. However, access to communications data is a contentious issue. Recognising this, on 15 October 2008, the then Home Secretary announced that a public consultation would be launched to develop the safeguards for the new system. The consultation document, entitled *Protecting the Public in a Changing Communications Environment,* was published in April 2009. It explained the vital importance of access to communications for the police and intelligence and security Agencies and others in safeguarding the public, the impact of the changing communications environment and the measures required to ensure that current capabilities are maintained into the future:

> *The Government believes it must take action to maintain the existing capability which is available to some public authorities. Doing nothing is not an option: crimes that are currently detected would not be detected in the future; lives that are currently saved may be lost.*[169]

Z. The Committee considers that continued investment in the Agencies' capability to access communications data and undertake lawful interception is essential to the national security of the UK.

---

[165] Intelligence and Security Committee Annual Report 2007–2008, *Cm 7542.*

[166] Protecting the Public in a Changing Communications Environment, *Cm 7586, April 2009, paragraph 11.*

[167] *Interception Modernisation briefing – 19 November 2008.*

[168] *Oral evidence – Home Secretary, 28 April 2009.*

[169] Protecting the Public in a Changing Communications Environment, *Cm 7586, April 2009, paragraph 14.*

Access to papers

183. We reported in our 2006–2007 Annual Report[170] on the Government's continued refusal to give the Committee access to a Ministerial submission in relation to a very serious allegation on which we took evidence in 2000. We have continued to request sight of the document as we believe it is a matter of principle that the Committee be given access to any documents that are relevant to its work.

184. The Prime Minister agreed at our meeting with him in February 2009 that this situation must be resolved, and as a result we have now been given sight of the document in question. We were reassured that the content of the document reinforced other evidence provided to the Committee at the time and, this being the case, we have now closed the matter.

[170] *Cm 7299, page 38.*

LIST OF WITNESSES

Ministers

The Rt. Hon. Jacqui Smith, MP – Home Secretary (until 5 June 2009)

The Rt. Hon. David Miliband, MP – Foreign Secretary

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Iain Lobban – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Scarlett KCMG – Chief, SIS (until 31 October 2009)

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 – Chair, Joint Intelligence Committee

Mr Chris Wright – Director, Security and Intelligence (until 28 August 2009)

Mr Tim Dowse – Chief, Assessments Staff (until 15 May 2009)

Mr William Nye – Director, National Security

Other officials

MINISTRY OF DEFENCE

Air Marshal Chris Nickols – Chief of Defence Intelligence (since January 2009)

Other officials

Defence, Press and Broadcasting Advisory Committee

Sir Bill Jeffrey KCB – Chairman (and Permanent Under Secretary of State, Ministry of Defence)

Mr Simon Bucks – Vice-Chairman and Chairman Media Side (and Associate Editor, Sky News)

Air Vice-Marshal Andrew Vallance CB OBE – Secretary

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 orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

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

TSO@Blackwell and other Accredited Agents

Customers can also order publications from
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401