



Intelligence and Security Committee

Annual Report 2006–2007

Chairman:

The Rt. Hon. Paul Murphy, MP

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
by Command of Her Majesty
January 2008

© Crown copyright 2008

The text in this document (excluding the Royal Arms and departmental logos) may be reproduced free of charge in any format or medium providing that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Any enquiries relating to the copyright in this document should be addressed to The Licensing Division, HMSO, St Clements House, 2-16 Colegate, Norwich NR3 1BQ. Fax: 01603 723000 or email: licensing@cabnet-office.x.gsi.gov.uk

From: The Chairman, The Rt. Hon. Paul Murphy, MP

**INTELLIGENCE AND SECURITY
COMMITTEE**

70 Whitehall
London SW1A 2AS

ISC 231/2007

4 December 2007

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

Dear Gordon,

I enclose the Intelligence and Security Committee's Annual Report for 2006–2007. In producing the Annual Report, we have examined and taken evidence on matters within our general oversight remit. This includes the policy, administration and expenditure of the three intelligence and security Agencies; the work of the wider intelligence community; and the ban on the use of intercept as evidence in court.

The Committee has held 49 formal sessions and 19 other meetings since we last reported in July 2006. In addition to this Report we have also spent a significant proportion of the year conducting a detailed inquiry into Rendition and our Report on this matter was published in July. We have also, since May this year, been carrying out a thorough investigation into the links between the CREVICE plotters and the 7 July London bombers, in the light of evidence that emerged from the CREVICE trial. We hope to report on this matter next year.

*Yours ever,
Paul*

PAUL MURPHY

THE INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Paul Murphy, MP (Chair)

The Rt. Hon. Michael Ancram QC, MP

The Rt. Hon. George Howarth, MP

The Rt. Hon. Alan Beith, MP

The Rt. Hon. Michael Mates, MP

Mr Ben Chapman, MP

Mr Richard Ottaway, MP

The Rt. Hon. Lord Foulkes of Cumnock
(since 7 February 2007)

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 and Government Communications Headquarters. The Committee has developed its oversight remit, with the Government's agreement, to include examination of the work of the Joint Intelligence Committee 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, part of the Ministry of Defence, which assists the Committee in respect of work within the Committee's remit.

The Prime Minister, in consultation with the leaders of the two main opposition parties, appoints the ISC members. 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(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.

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

CONTENTS

THE INTELLIGENCE AND SECURITY COMMITTEE	iv
GLOSSARY	2
INTRODUCTION	3
Work programme.....	4
Proposed reform of the Intelligence and Security Committee	5
THE AGENCIES	6
Single Intelligence Account	6
Security Service	7
Secret Intelligence Service.....	10
Government Communications Headquarters	15
Value for money and efficiency in the Agencies	19
Media relations.....	20
THE INTELLIGENCE COMMUNITY	22
Permanent Secretary, Intelligence, Security and Resilience	22
Joint Intelligence Committee and Assessments Staff.....	22
Professional Head of Intelligence Analysis.....	23
Defence Intelligence Staff.....	23
SCOPE	25
Serious Organised Crime Agency	26
The Commissioners.....	27
Review of counter-terrorism strategy.....	27
Official Secrets Act	29
OTHER ISSUES	30
Investigation into BAE Systems.....	30
Intercept as evidence	32
ANNEX A – REFORM OF THE ISC.....	35
<i>The Governance of Britain</i> Green Paper	35
Parliamentary debate.....	37
ANNEX B – ACCESS TO PAPERS	38
SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS.....	39
LIST OF WITNESSES	42

GLOSSARY

CDI	Chief of Defence Intelligence
CESG	Communications Electronic Security Group
CONTEST	UK Counter-Terrorism Strategy
CSR07	Comprehensive Spending Review 2007
CT	Counter-Terrorism
DCDI	Deputy Chief of Defence Intelligence
DIS	Defence Intelligence Staff
FCO	Foreign and Commonwealth Office
GCHQ	Government Communications Headquarters
HMRC	HM Revenue and Customs
ISC	Intelligence and Security Committee
IT	Information Technology
JARIC	Joint Air Reconnaissance Intelligence Centre
JIC	Joint Intelligence Committee
MoD	Ministry of Defence
NAO	National Audit Office
NIO	Northern Ireland Office
PFI	Private Finance Initiative
PHIA	Professional Head of Intelligence Analysis
SIA	Single Intelligence Account
SIC	Security and Intelligence Co-ordinator
SIGINT	Signals Intelligence
SIGMOD	GCHQ's SIGINT Modernisation programme
SIS	Secret Intelligence Service
SOC	SCOPE Service Operations Centre
SOCA	Serious Organised Crime Agency

INTRODUCTION

1. There remains a serious and sustained threat from international terrorism to the UK and its interests overseas, the most significant being from al-Qaeda and associated networks. The period since we last reported has seen an exceptional workload for the intelligence and security Agencies, whose focus has been, of necessity, on countering this threat.¹ The Agencies and police have successfully disrupted a number of terrorist plots, including the alleged airliner bomb plot in August 2006, and the alleged plot to abduct and murder a British Muslim soldier in the West Midlands in February 2007. This year has also witnessed the successful convictions of five men involved in a plot to detonate a fertiliser bomb in 2004, seven men involved in attack planning associated with Dhiren Barot, four men who attempted bomb attacks on the London transport system on 21 July 2005, and three men for incitement to murder (the first convictions of this type for internet-based extremism). These plots serve to underline both the seriousness and the scale of the terrorist threat the UK is facing.

A. We would like to record our thanks and praise to the staff of the intelligence and security Agencies, as well as the police and our overseas partners, for all their hard work.

2. Recent attempted attacks have shown that, despite the hard work of the Agencies and the increased resources at their disposal, there is no guarantee that attack planning will be detected, or that attacks will be prevented. To give an idea of the scale of the threat, there are approximately 200 extremist networks currently under investigation, some of which have both the intent and capability to carry out attacks against the UK or UK interests overseas. There will be still others about which little or nothing is known.

3. The Committee recognises the need to focus on the terrorist threat. We note, however, the proportionate reduction in resources dedicated to tackle other areas. These include:

- ***
*** (in the case of the Security Service);
- ***
*** (for the Secret Intelligence Service (SIS)); and
- ***

*** (in the case of Government Communications Headquarters (GCHQ)).

The Security Service told the Committee:

I think the scale of the international terrorist threat at the moment is such, and the consequences if we are unable to manage it successfully nationally I think are so severe, that we have not had any choice but to prioritise [over other] areas.

¹ The Committee last reported in July 2006. This Report covers matters up until October 2007.

Some of the changes I suspect probably will not quickly reverse. I suspect we will be quite slow to get back into serious crime work, for instance... [On areas] such as counter-espionage, I think we have to continue to look at this on a fairly regular basis.²

B. We are concerned that aspects of key intelligence and security work are suffering as a consequence of the focus on counter-terrorism priorities. We believe consideration may need to be given to separate, additional funding to maintain the Agencies' capabilities in these areas.

Work programme

4. The Committee has held 49 formal sessions and 19 other meetings since we last reported in July 2006. During this time, we have conducted three major strands of work:

- A significant proportion of the year was spent conducting a detailed inquiry into Rendition – our Report on this matter was published in July.
- In May this year the Prime Minister asked the Committee, and the Committee agreed, to examine the links between the CREVICE plotters and the 7 July London bombers, in the light of evidence that emerged from the CREVICE trial. We are carrying out a thorough and wide-ranging investigation, re-examining earlier evidence and holding new evidence sessions.
- We have also examined and taken evidence on matters within our general oversight remit. This includes: the policy, administration and expenditure of the three intelligence and security Agencies; the work of the wider intelligence community; and the ban on the use of intercept as evidence in court.

5. Those we have taken evidence from in connection with the above include the Foreign Secretary, the Home Secretary, the Attorney General, the Independent Reviewer of Counter-Terrorism Legislation, senior members of the West Yorkshire and Metropolitan Police Services, and senior officials including the Cabinet Secretary, the Permanent Secretary, Intelligence, Security and Resilience, the Heads of the Agencies, the Chief of Defence Intelligence and the Head of the Serious Organised Crime Agency (SOCA). The Committee also held a seminar to consider radicalisation and ***. We also held informal discussions with the Interception and Security Services Commissioners.

C. We wish to note that whilst the Agencies themselves handle the Committee's requests for information promptly, our work this year has been hampered on occasion by government departments failing to keep the Committee formally informed of changes relevant to its work.

6. As part of the Committee's programme of reviewing different oversight systems, we attended:

- the International Intelligence Review Agencies Conference held in South Africa;

² Oral evidence – Security Service, 16 January 2007.

- the Conference of the Parliamentary Committees for the oversight of intelligence and security services within the European Union held in Romania; and
- the International Symposium on intelligence oversight hosted by the Netherlands.

In terms of bilateral discussions, we visited the United States and hosted visitors from Argentina, Australia, Canada, Slovenia and Switzerland.

7. ***

 ***.

Proposed reform of the Intelligence and Security Committee

8. The Prime Minister's Green Paper on *The Governance of Britain* contained suggestions as to how this Committee might be strengthened to maximise the effectiveness of its scrutiny role, whilst reinforcing its relationship with Parliament. Extracts from the Green Paper and relevant statements in Parliament are included at Annex A.

9. We welcome moves to improve accountability of this Committee to Parliament. The work of the Committee has grown and developed since its inception in 1994; after 13 years it is right to take stock and consider whether the legislation accurately reflects the remit and powers of the Committee, and whether change is now needed in the new post-9/11 and 7/7 world. We have formulated our proposals to ensure that the Committee continues to provide effective oversight of our intelligence and security Agencies, and have submitted these to the Prime Minister.

10. One of the areas under discussion is that of access to sensitive documentation. The legislation currently allows for the most sensitive material to be withheld from the Committee at the discretion of the Heads of the Agencies or the Home Secretary or Foreign Secretary. We note that, since the Committee was formed in 1994, there has only been one case in which access to papers has been requested and refused. This has been detailed in Annex B to this Report. The Committee believes that, particularly in light of its recent enquiries into Rendition and the links between the 7 July bombings and the fertiliser bomb plot, it is vital that it can have access to relevant documentation, where necessary.

THE AGENCIES

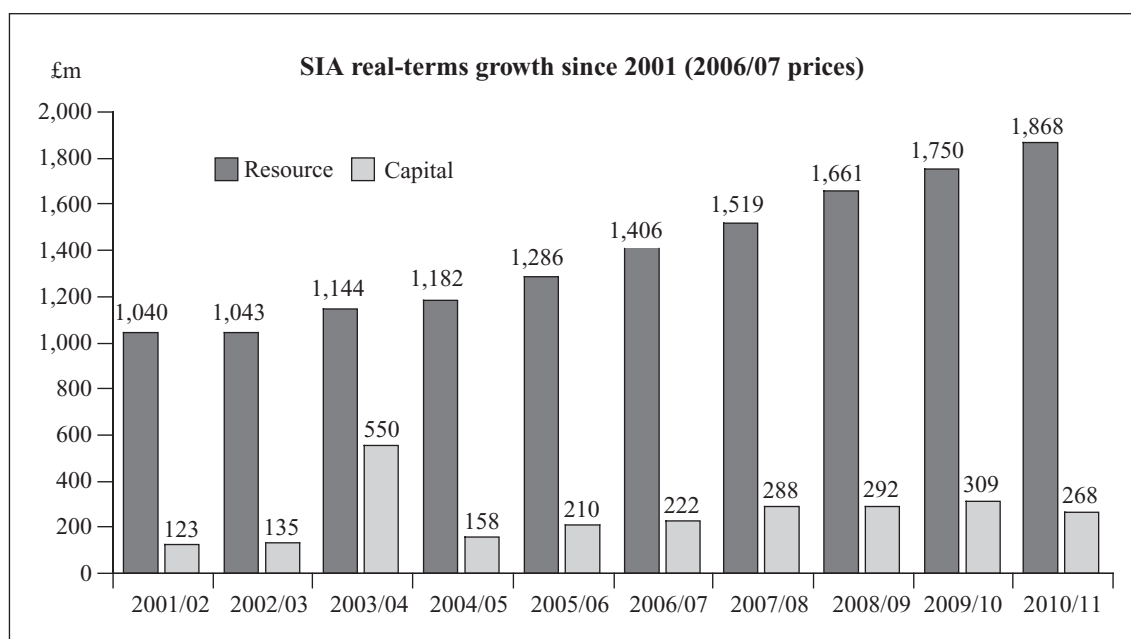
Single Intelligence Account

11. 2006/07 saw a further increase in the Single Intelligence Account (SIA), from which all three Agencies are funded. This was in addition to the £85 million made available over three years (2005/06 to 2007/08) by the Chancellor in his 2005 Pre-Budget Report.

12. In his Budget Report to the House of Commons on 21 March 2007, the Chancellor announced a further £86.4 million for the Agencies to accelerate the development of their counter-terrorism capabilities. It is hoped that the extra resources will strengthen partnerships between the Agencies and the police, and improve data exploitation capabilities.

13. The Chancellor announced the outcome of the 2007 Comprehensive Spending Review (CSR07) in October 2007. The settlement for the CSR07 period provides a total Departmental Expenditure Limit (resource plus capital net of depreciation) for the SIA of £1,855 million, £2,009 million and £2,147 million for 2008/09, 2009/10 and 2010/11 respectively. This represents a substantial real-terms increase in budget and demonstrates a commitment on the part of the Government to continue efforts to build counter-terrorism capacity in the Agencies.

14. The chart below illustrates the real-terms growth in expenditure for the Agencies over the decade since 9/11 (based on 2006/07 prices).³



³ The chart shows actual expenditure up to 2006/07, predicted expenditure for 2007/08 and planned expenditure for 2008/09 to 2010/11 (as agreed at CSR07). The high capital figure in 2003/04 reflects a one-off spend on new accommodation. The figures have been adjusted to 2006/07 prices to enable a more appropriate comparison.

15. The following table shows the actual and predicted expenditure for the period 2005/06 to 2008/09.⁴

Expenditure in millions (£)		Actual 2005/06	Actual 2006/07	Predicted 2007/08 ⁵	Planned 2008/09 ⁶
SIA total⁷	Resource	1,251.2	1,405.5	1,570.3	1,765.0
	Capital⁸	204.1	221.8	297.3	310.0
SIA level adjustments ⁹	Resource	—	***	***	***
	Capital	—	***	***	***
GCHQ	Resource	***	***	***	***
	Capital	***	***	***	***
SIS	Resource	***	***	***	***
	Capital	***	***	***	***
Security Service	Resource	***	***	***	***
	Capital	***	***	***	***

D. We welcome the increase in the Single Intelligence Account for the next three years: it responds to the increased scale of the threat, and the growth of the work needed by the Agencies to counter it. The Committee intends, in the coming year, to investigate the allocation of the increased CSR07 settlement between the three Agencies and the associated spending plans.

Security Service

16. The Security Service Resource Account for 2005/06 was agreed by the Comptroller and Auditor General in July 2006. The Service increased its spend during 2005/06 by nearly 29% against 2004/05, spending around £*** against £*** the previous year.

Counter-terrorism

17. The Service received £*** over three years from the November 2005 Pre-Budget Report and a further £*** from the £86.4 million announced by the Chancellor in March 2007. These additional funds will be used to strengthen counter-terrorism capability and to sustain the current intensive operational effort. It will also fund intelligence collection and surveillance improvements, including *** against difficult targets.

⁴ The Committee considers in detail the approved accounts for the Agencies. Due to the timing of Reports, the Committee always considers the previous year's accounts. Therefore, for this 2006–2007 Annual Report, the detail is given on the 2005/06 accounts. The table shows actual expenditure up to 2006/07, predicted expenditure for 2007/08, planned expenditure for 2008/09, and includes the Pre-Budget Report 2005 settlement.

⁵ Funding in 2007/08 includes additional counter-terrorism funding announced in Budget 2007.

⁶ The planned expenditure figures for 2008/09 include the CSR07 settlement. Individual Agency allocations for 2008/09 are provisional.

⁷ SIA totals include funding for the ***.

⁸ The capital figures refer to net cash expenditure on fixed assets.

⁹ The SIA "level adjustment" in 2006/07 is an end-of-year accounting adjustment on consolidation. The level adjustment for 2007/08 includes central funding for SCOPE, Information Assurance and BBC Monitoring.

18. In March 2006, the Service was allocating 53% of its operational effort (around £*** of resource) to international counter-terrorism (an increase of 11% on the previous year), and 14% to protective security (largely related to international counter-terrorism work). Subsequently, the former Director General updated this, saying:

*We have agreed a package of measures that will increase [international counter-terrorism] to around 80% of our total (currently 70%) effort through the reallocation of over 100 existing and newly recruited staff. This will be achieved through a reduction in [other areas of] work... [which is not] welcome, but the *** OVERT and its strategic significance compels us to make hard choices...*¹⁰

19. The Committee recognises the scale of the challenge the Service is facing (the Service currently has around 200 networks – some 2,000 individuals – under investigation) and agrees on the need for additional funding. It is, of course, important that the funds are spent in the right way and that they are maximising the Service’s capability. When questioned on the impact of the budget increase, the former Director General said:

***¹¹

Administration

20. The former Director General told us “my main concern has been, and still is, we do not have enough people to do the job”.¹² Therefore, with these increased resources at its disposal, the Service has run an ambitious recruitment programme. At the time of publication, the total number of staff in the service is around 3,200, with a further 690 individuals (including in Northern Ireland) due to be recruited over 2007/08.

21. There are a number of risks associated with significant expansion programmes. One of these is the possible reduction in the overall quality of personnel – a case of quantity rather than quality. The former Director General was, however, clear that standards must be maintained:

[Maintaining standards] is incredibly important because people get access to secrets and responsibility and the capacity to make a major [mistake] very early on.

*That is always a strain upon faster growth. When I am criticised for not growing faster than we have, there is a balance to be struck here. At the moment we are able to attract very high calibre recruits and I hope that will last. We can be extremely choosy about who we take and good people are joining us.*¹³

22. One of the results of the ambitious recruitment programme is an increased demand for training. The Service launched its training academy in January 2006 to boost levels

¹⁰ Letter from the Security Service, 16 October 2006.

¹¹ Oral evidence – Security Service, 16 January 2007.

¹² Ibid.

¹³ Ibid.

of learning and development activity and improve the quality of training provision. The academy delivers a structured and flexible curriculum that ensures training is tailored to the skills requirements of the Service and its business. A formal mentoring scheme has also been introduced to facilitate the smooth introduction and development of newly recruited staff into their teams.

23. Another risk of expansion on which we commented in our last Annual Report is the possible inability of corporate services to keep up with the growth of the organisation as a whole. The Service has recognised this risk and has embedded project management capabilities in its capacity-building projects to ensure that this risk is minimised. Capacity-building projects taken forward during 2006/07 include: improving support to the surveillance fleet; overhauling the Service's secure communications network; and further developing the Service's ability to exploit information in support of operations.

24. Further administrative improvements include a major new £*** software application project to overhaul the Service's human resource, finance and reporting functions. Based on existing, off-the-shelf software, the programme will offer a computer and database management facility on which much of the Service's administrative, corporate, and financial planning will depend. The former Director General said:

*[It] is a project that we believe is overdue to help us run all the things to do with a much bigger workforce; in other words, using it to map skills, promotions, transfers, expenses, etcetera. We have systems for all of that but they are old systems. They make it difficult for a senior manager to pull all that information together.*¹⁴

E. The Committee is reassured that the Security Service is managing to minimise the risk that inevitably accompanies a rapid growth in staff numbers.

25. We note, however, that the Service used significantly more consultants during 2006/07 – spending around £*** on work on information technology (IT) development and buying in project management skills. The former Director General acknowledged that this was not ideal but said there had been no other option to ensure that the Service delivered the capabilities required to meet the threat:

*Faced by a very significant gap between the scale of the problem we are addressing and the people to address it, we have used consultants to do some things which might previously be done by staff. This is expensive, but we have done this consciously because of the requirement really to do a great deal of energy on the operational side.*¹⁵

The Service told the Committee that it intends to provide greater detail on spending on consultants, and what they have delivered, in next year's accounts and we will return to the matter then.

¹⁴ *Ibid.*

¹⁵ *Ibid.*

Northern Ireland

26. On 10 October 2007, the Security Service assumed the lead role for national security in Northern Ireland (as part of the process of normalisation of policing and security with the rest of the UK). The Service's new headquarters in Belfast (known as Loughside) was completed on time and within the £*** budget. Loughside is part of the Service's regionalisation strategy and also provides an important contingency capability in the form of a back-up for Thames House.

27. Last year, the Committee expressed concern that funding arrangements for national security in Northern Ireland had not yet been agreed between the Service, the Northern Ireland Office (NIO), the Ministry of Defence (MoD), and the Treasury. Since then, negotiations have been successfully concluded. The NIO has agreed a transfer of £*** per annum and the MoD a transfer of £*** per annum. The CSR07 settlement for the Security Service includes these sums. The Committee has also been told that formal agreements are now in place between the Service and its partners in Northern Ireland and that these cover the provision of staff, funding, surveillance support, and other resources to the Security Service.

Regionalisation

28. The Service has continued its regionalisation programme this year. Its presence in the Midlands, North East, North West, South, East and Scotland grew in 2006/07 and new offices were opened in the South East and Wales during this period. By 2008, regional stations will house three times the number of staff originally planned.

29. We have been told that close liaison with police forces has enabled the stations to make a significant contribution to counter-terrorism work. The nine arrests in Birmingham at the beginning of February 2007 are an example of where the regional capability of the Service has greatly helped police to carry out counter-terrorism operations. The former Director General said during the case:

It is clear to me that having an established station in [the West Midlands] that is able to work very closely with both the Special Branch and the CT unit in [the West Midlands] on this case is extremely helpful for coordination which involves also the Met. So having that sort of coordinating function... is of real value.¹⁶

F. The Committee has been impressed by the speed at which the regionalisation programme has been carried out and the clear benefits it has brought.

Secret Intelligence Service

30. The SIS 2005/06 Resource Account was agreed by the Comptroller and Auditor General in July 2006. SIS spent £*** of resource over 2005/06, an increase of 3.6% over the previous year. (This contrasts sharply with the Security Service whose expenditure increased by nearly 29% over the same period.)

¹⁶ *Ibid.*

31. Much of the £*** additional funding allocated to SIS in the 2005 Pre-Budget Report was used to enhance front-line counter-terrorism operations overseas – particularly in *** – and to develop the capacity of liaison services in priority countries. This work has continued through 2006/07 and has included projects in ***, ***, ***, ***, *** and *** with further capacity-building work planned in key areas of the *** region and the ***. The funding has also enabled SIS to put more personnel on the ground in areas where British forces are operating. The Service’s £*** share of the further £86.4 million announced by the Chancellor in March 2007 will be used to improve the intelligence picture of the links between overseas and UK-based terrorist networks.

Counter-terrorism

32. SIS reprioritised its resources after the London bombings in July 2005 to provide a greater focus on the international dimensions of terrorism. Operation OVERT (the summer 2006 alleged airliner bomb plot) – with which SIS was heavily involved – led to an acceleration of this work. Changes have included a reduction in *** work in ***; a reduced number of operations in the *** region; the closure of two stations in ***; the transfer of serious crime work to SOCA; and the suspension of operations directly related to economic wellbeing.

33. The resource released by these changes has enabled SIS to strengthen its coverage and operational capability in key aspects of international counter-terrorism:

*We are now engaged in a range of counter-terrorism work; direct pursuit of terrorists, ***, capacity-building with key [countries,] and – this is an absolutely vital point – ***. ***. ***. So put like that and defined like that, this takes up about 56 per cent of our effort... and it is rising.¹⁷*

34. SIS has improved its *** and its understanding of the factors that have the potential to affect radicalisation and extremism in the UK. The Chief of SIS told the Committee “we have to think creatively”.¹⁸ He said that a specialist operational team had been created within SIS:

*to illuminate... the interface between al-Qaeda and radicalised British Muslims, essentially to catch the connection between... the domestic aspect of the threat and the overseas aspect of the threat ***.¹⁹*

35. A further change is the increased proportion of SIS’s total operational front-line staff now working in joint operational teams with the Security Service. This has increased by a further 4% against 2005/06.

¹⁷ Oral evidence – SIS, 23 January 2007.

¹⁸ *Ibid.*

¹⁹ *Ibid.*

36. SIS's greater focus on counter-terrorism has led to a significant increase in the number of direct "disruption operations" against terrorist targets throughout the year. The total number of these operations has increased by almost 50% compared with the previous year, and the number of these operations judged to have caused "significant disruption" to the terrorist targets has almost doubled.

Non-counter-terrorism work

37. With the formation of SOCA, SIS has been able to withdraw from some of its non-counter-terrorism responsibilities. One of the areas in which SIS has retained a significant interest is counter-narcotics work – both in areas where it is closely linked to SIS's counter-insurgency work (for example, in ***), or where it is of such political value to partner countries that withdrawal could undermine SIS's wider relationships with the intelligence and security services of those countries (for example, in ***).

38. Where operations are linked to counter-insurgency, SIS has continued its levels of activity and investment, with very limited involvement from SOCA. Where SIS judges that withdrawal would have political consequences for wider relationships, SIS is aiming to maintain the overall political management and control of the more sensitive operations, whilst transferring day-to-day practical management to SOCA, the police or HM Revenue and Customs (HMRC), thus lowering the investment but maintaining a strategic interest. Speaking of this latter type of operation, the Chief of SIS told the Committee:

We have had a heavy SIS investment... and remarkable success for that investment. We have become deeply involved in the setting up and management of quite complex... operations. Now these have been established, there clearly is an argument for saying "well, the management and running of these is not something which naturally falls to SIS. It is certainly something which could in theory be done by SOCA."

At the same time, they are so important, they achieve such results, they have such a strategic impact, and therefore they have such a political profile that they are not just police operations. They have real political and strategic significance. For us to just pull out of them would risk, first of all, undermining the bilateral relationship quite seriously... and secondly, cause them maybe to lose their strategic focus...

If you succeed in taking down a major figure or a major network or a major... agro-industrial combine which is at the centre of massive money laundering and drugs related activity, then you can begin to think that you are having some strategic effect.²⁰

39. SIS is also maintaining and reinforcing its work on other non-terrorism-related threats to British interests. The Chief of SIS told the Committee:

*On ***, that has been effective and it is a good story. On ***, it is getting better but we need to do more. Again, it is a key point in terms of the management of the Service. We are able to identify and resource, although not always as much as I would like, major intelligence issues and targets which are separate from the drive on CT...*

²⁰ *Ibid.*

*The *** have reminded us *** we need to worry about *** too. I do not need to argue that case anymore in the way that I had to in the past... In fact we manifestly need to reinforce our efforts against these sorts of issues.²¹*

Administration

40. In SIS's 2005/06 accounts, the National Audit Office (NAO) had highlighted two cases where there had been errors in the reporting of payments made to agents (this problem had also been uncovered by SIS's own internal audit procedures). The problem was associated with incomplete "contact reports" which should record, amongst other things, any cash or benefits provided to the Service's agents from public funds. The Chief of SIS told the Committee:

It is that the audit trail that lay in place was not as good as it should have been because payments made to agents, which should have been recorded in substantive contact reports, were not, because the contact reports were not completed...

So in effect, we had an incomplete record of dealings with agents and a compromised audit trail in an area where we really do not want it. Clearly, we have got to be completely confident in that particular area that we have got the trail really tied up.

41. In response to questions as to what was being done to resolve the problem and ensure that it did not happen again, the Chief of SIS told the Committee:

We have made quite an issue of this internally. We have... republished the standing instructions and we have re-emphasised regularly in all operational training courses and briefings the absolute importance of ensuring the contact notes are always completed... We have also got budget managers carrying out regular checks of contact reports to confirm that the payment details are correctly reported. So we have a checking system in place.²²

G. Payments from public funds, including payments to agents, must be properly managed and recorded. We are pleased that steps have been taken by SIS to correct this problem and will monitor compliance and accuracy levels in the future.

42. During 2006, SIS has made some changes to its organisational structure, which was in danger of becoming outdated as the challenges it faces evolved. SIS has realigned its internal "Controllerate" divisions to reflect new priorities. In some areas, this will involve a ***. These changes build on the new arrangements for the recruitment and management of operational officers (discussed in our 2005–2006 Annual Report) which have generated a larger and more flexible pool of operationally deployable staff. The forthcoming year will be the first test of these new arrangements.

²¹ *Ibid.*

²² *Ibid.*

43. SIS currently has around *** permanent staff, with a projected growth of about 5% per annum.²³ Although the Service is not growing as dramatically as the Security Service, the changes discussed above – and the increasing ratio of new to experienced staff – still pose a risk to the corporate culture of the organisation. The Chief of SIS told the Committee:

Any growth carries risk, particularly to a sensitive sort of delicate structure and system like ours... at the end of, let's say [the next] five year period, a substantial proportion of the Service's staff will be quite inexperienced... and there will be a disconnect between that inexperience and then the ability of the more experienced part of the Service to manage that and to control it and to direct it. And obviously a Service like ours cannot afford to flip-flop around with weak management, particularly middle management, which is where the risk is likely to be most intense...

I have to say, I am less worried about it this year than I would have been last year... And that is based upon what I have seen of our ability to grow and absorb staff in the intervening period. We are getting better at it... So I am more comfortable about that than I was, but we have to watch it very carefully.

In terms of the actual culture of the Service... again, I think that we can manage that. The culture in the Service is extremely strong and I find that most people coming in are very ready to take much of it on.²⁴

44. A staffing issue that remains concerning, however, is that of retirement ages. The Civil Service retirement age is due to increase to 65 over the coming years. The Committee touched on the issue last year and returned to it again this year, asking the Chief of SIS about the implications of this for SIS staff. We were told that, should this change be implemented in SIS, it could pose problems in terms of overseas deployment of staff and effective intelligence gathering, but that the matter would be kept under review.

45. Another issue the Committee returned to this year is that of business continuity – in particular, the Committee discussed SIS's arrangements for backing up its data. The Committee has been told that the Service's ***. We last discussed this matter with the Chief of SIS in January 2007 and, at that stage, a more secure and modern solution to these – in our view – unsatisfactory arrangements had still not been implemented.

H. We conclude that there has been a lack of progress regarding the business continuity of SIS system back-ups. We also note that issues surrounding SIS's retirement age and pensions policy appear to have not yet been resolved. The Committee recommends that these matters are now given a greater priority.

²³ This number includes ***.

²⁴ Oral evidence – SIS, 23 January 2007.

Government Communications Headquarters

46. In 2005/06, GCHQ's net operating costs rose to £*** – an increase of 11.7% against 2004/05. Its Resource Account was agreed by the Comptroller and Auditor General in July 2006, and the NAO has noted that GCHQ continues to build its track record of accounting excellence. GCHQ was also allocated an additional £*** in the 2005 Pre-Budget Report.

47. GCHQ's £*** share of the further £86.4 million announced by the Chancellor in March 2007 will be channelled predominantly toward additional recruitment in key areas. Reflecting the need for ever-closer working on counter-terrorism operations, the funding will enable GCHQ to deploy more analysts into the Security Service and other partners working on counter-terrorism. The additional funding will also be invested in enhancing their technical capabilities in areas such as target discovery and the internet.

Counter-terrorism

48. Recognising a need to strengthen its counter-terrorism capabilities, GCHQ reallocated resources throughout 2005/06 to cover terrorist targets. This work was often manifested through direct support to key Security Service investigations – notably OVERT, for which GCHQ temporarily diverted significant resources to support the operation. The Director explained the close correlation between GCHQ's work and that of the Security Service:

How much we need to grow will depend more or less on how much ministers decide to grow the Security Service. So our CT capability will need to keep pace so we can support the number of operations there that they are running... By the end of the year we had found that we were managing to support most of Security Service's highest priority operations, but we were not achieving the quality of support that we and they had agreed we should aim for... essentially because we were spreading ourselves too thin... We do not have enough CT resources.²⁵

I. The substantial growth in the number of Security Service counter-terrorism operations in recent years has made it difficult for GCHQ to maintain high-quality support to an ever-growing number of investigations. We will monitor the impact of the CSR07 settlement on resolving this problem.

²⁵ Oral evidence – GCHQ, 30 January 2007.

Technological change

49. One of the greatest challenges for GCHQ is to maintain its intercept capability in the face of rapidly evolving communications technology. This relates in particular to the growth in internet-based communications and voice over internet telephony. The Director explained the significance of these changes:

The Internet uses a very different approach to communications in that, rather than having any sense of fixed lines like that, there is a big network with a number of nodes, but for any individual communicating, their communications are broken up into shorter packets. So whether you are sending an email or any other form of Internet communication, anything you send is broken up into packets. These packets are then routed around the network and may go in any one of a number of different routes because the network is designed to be resilient...

This [represents] the biggest change in telecoms technology since the invention of the telephone. It is a complete revolution...

***²⁶

50. The seriousness of these challenges was reinforced by the Director General of the Security Service, who told the Committee:

***²⁷

51. In our 2005–2006 Annual Report, we commented on GCHQ’s SIGINT Modernisation (SIGMOD) programme – the collective name for projects that represent the work needed to keep GCHQ ahead in the SIGINT business. Given the speed at which technology develops, an organisation like GCHQ must reinvest continuously to keep up with the methods that are used by those who threaten the UK, both at home and overseas. GCHQ plans to spend around £*** over three years on SIGMOD.

52. A key requirement for the SIGMOD programme is to deliver the improvements in GCHQ’s technological capability to address the challenges of increasing internet communications over the coming decade – including ***. The Committee has taken detailed evidence on these problems, and GCHQ’s efforts to overcome them.

²⁶ Oral evidence – GCHQ, 8 March 2007.

²⁷ Oral evidence – Security Service, 16 January 2007.

53. Over the last two years, SIGMOD has delivered:

- a twentyfold increase in GCHQ's ability to access, process and store ***;
- an increased ability to store ***;
- improved connections between GCHQ databases and those of the Security Service and SIS to allow analysts to work collaboratively and share data; and
- an applications hosting service to provide greater flexibility and efficiency to GCHQ's software developers.

54. SIGMOD has also provided further improvement in the automation of certain aspects of the analysis of communications, allowing improved identification of networks – a task that previously had to be performed manually. As a result, analysts now have more time to interpret the data and establish its significance. Also, the SIGMOD programme has contributed to improvements in a wide range of collection capabilities, ***.

J. The Committee is satisfied that, despite the substantial costs involved, the current SIGINT Modernisation programme represents an essential investment in maintaining GCHQ's technological capabilities. Given the unremitting progress of technology – particularly internet-based communications – we believe it is vital that plans and budgets are established early to ensure that GCHQ is able to continue vital modernisation work. The Committee will continue to monitor the existing programme and intends to study these future plans carefully.

Support to military operations

55. Another priority for GCHQ has been the continuing support to military operations in ***, and there were some notable successes over the year as, by using a range of specialist collection systems, GCHQ was able to provide customers with insight into ***. Some of this work has required more GCHQ staff to be deployed to military headquarters overseas.

Administration

56. The complex challenges of SIGMOD and the vast sums of money involved illustrate the importance of procurement to GCHQ. GCHQ's Finance Director said:

*I would say procurement is one of the most significant challenges GCHQ has had and will, to be honest, continue to have over the next several years. The size of investment spend we have every year, the size of procurement we do, in excess of £*** worth of IT related procurement every year, it has to remain a key area of focus for us.²⁸*

²⁸ Oral evidence – GCHQ, 30 January 2007.

57. In previous years, the NAO has expressed concern that GCHQ had struggled to meet standards in best practice and achieve value for money across “whole-life costs” of contracts and purchasing. GCHQ has made several changes to address these criticisms. It has established a dedicated oversight body within the organisation to examine the whole end-to-end procurement cycle. This group reports to GCHQ’s Head of Technology, with governance provided by the Finance Director. The group has agreed targets for procurement savings and these are on track to be delivered this year, with a saving of around £*** thus far. GCHQ has also recruited a contract management specialist, and has put mechanisms in place to provide an independent assessment of the status of key contracts. Separately, the organisation is developing longer-term relationships with key IT suppliers, made necessary by its increasing commitments to long-term contracts. Finally, GCHQ’s procurement function has obtained its Chartered Institute of Purchasing and Supply Standards Certificate – demonstrating that its purchasing and supply management operations have reached a nationally accredited level.

58. Another key financial issue for GCHQ is accommodation. In our 2005–2006 Annual Report, we noted a continuing issue over occupancy and ownership of GCHQ’s old Oakley site in Cheltenham. In commissioning a new building, GCHQ’s original requirement was for accommodation for around 4,000 staff, but the demand for SIGINT services post 9/11 has driven growth of the organisation to a level for which the new building was not designed. At the same time, the original private finance initiative (PFI) agreement required a full exit from the old site by 2012. In 2005, the Board considered two options to manage this problem: to complete the planned exit of the site on Oakley by 2012, and build further accommodation within the new site; or to renegotiate the agreement with the PFI companies (GSL and Wimpey) to extend their occupancy of the old site by five years to 2017.

59. Possible further increases to GCHQ’s headcount (as a result of OVERT, Security Service expansion, and CSR07) would validate a decision to retain the old site until 2017. GCHQ staff in 2005/06 comprised *** individuals, including Communications Electronic Security Group (CESG) personnel, and this number was projected to grow by about 6% in 2006/07 to meet an increasing need to support Security Service counter-terrorism operations, and growing demand for CESG’s services and expertise. Further growth in the Security Service as a result of CSR07 is likely to have a direct impact on demand for GCHQ’s services, creating a requirement for increased staffing levels and a concomitant pressure on existing accommodation.

60. After taking into account these factors and the financial risks they involve, including the future cost of borrowing, the Board decided to seek to extend their occupation of the old Oakley site. They felt that this entailed fewer risks to GCHQ’s business continuity, and would carry lower real-terms costs.

61. After negotiations with the PFI contractors, GCHQ agreed a £*** deal in February 2007 to repurchase the site. This decision will resolve the short-term pressure on accommodation space and gives GCHQ the ability to decide on what role, if any, Oakley will play in its longer-term accommodation strategy.

K. We conclude that, in the circumstances, GCHQ has handled its accommodation problem effectively and achieved the best value for money for the taxpayer in the short term.

62. The summer floods in the Gloucestershire region caused significant disruption to GCHQ and its staff. Despite some serious problems in unprecedented conditions, GCHQ was able to maintain its most important operations and we commend management and staff for the tenacity and dedication they demonstrated during such a difficult period.

L. We are very concerned that, had the flooding continued for very much longer or been more severe, GCHQ's operations could have been even more severely disrupted. In light of these events, the Committee intends to undertake a review of business continuity arrangements for all three Agencies in the coming year.

Value for money and efficiency in the Agencies

63. The significant additional funding made available to the Agencies since 9/11 has been accepted as essential for building capacity across the intelligence community to counter threats from international terrorism and provide a greater standard of coverage and assurance. It is important, however, that the considerable sums of money being channelled into the Agencies are well spent, appropriately controlled and monitored.

64. Like other Whitehall departments, the intelligence and security Agencies have a number of common efficiency objectives, which include targets laid down by the Gershon Review, and an additional 1% savings objective set by the Security and Intelligence Co-ordinator.²⁹ In addition, each Agency also has a set of internally agreed objectives with respect to efficiency and value for money.

65. The Security Service has a specific Public Service Agreement for efficiency, which includes a target to generate £*** of cost savings by March 2008. It is on track to meet this. The Service closely follows guidelines laid down by the Office of Government Commerce for measuring value for money, especially on areas like procurement, where each project is reviewed on a case-by-case basis. The Service achieved its 2004 Spending Review target of £*** for efficiencies through several means, including the professionalisation of its procurement function, and by keeping the headcount down in key support areas such as human resources and finance. Greater information exploitation has enabled the Service to run operations at a pace and volume that it would not have been able to undertake previously. In 2006/07, the Service's efficiency target was £***, but the Service actually identified an additional £*** worth of efficiencies. It is currently agreeing further efficiency targets for the 2007 Spending Review period with the Treasury.

²⁹ These efficiency objectives related to the 2004 Spending Review. New targets will be set for the CSR07 period.

66. SIS exceeded its efficiency target set during the 2004 Spending Review, making significant savings on procurement, travel costs, and the ***. As part of CSR07, SIS has worked with the Treasury to identify savings across a number of areas worth around £35 million. Any efficiency found in the corporate services functions, however, will be used to free up resource for front-line operational work. Like GCHQ and the Security Service, SIS sees procurement policy as a major opportunity to generate further efficiencies and, during 2006, has implemented new strategic partnership agreements with IT suppliers and has taken on additional qualified procurement professionals. Separately, SIS now has a dedicated Efficiency Officer, and a Contracts Management Officer who manages the Service's relationship with all self-employed contractors.

67. GCHQ faces perhaps a more difficult task when looking for efficiencies because its capital costs are high (and in a lot of cases fixed), its assets depreciate rapidly, and specialist technical support is not always available in house, requiring the use of expensive consultancy services. Nevertheless, GCHQ has fulfilled its efficiency and value for money requirements set in the 2004 Spending Review, and has generated an additional £*** worth of savings over and above these targets. Separately, GCHQ's Finance Director has put in place an aggressive internal efficiency target of 5% savings year on year in response to a need, like SIS, to transfer resources from corporate support areas to front-line operational requirements. This target represented about £*** of cash savings across 2005/06 and 2006/07, which was achieved. GCHQ is also in the process of agreeing its CSR07 efficiency target, which is expected to be about £*** over the CSR07 period.

Media relations

68. A continuing concern for the Committee is the increasing number of inaccurate and misleading reports in the media relating to the work of the intelligence and security Agencies, and the reporting of leaked and sensitive intelligence.³⁰ In some cases, this reporting has come close to compromising counter-terrorism operations; in others it has risked prejudicing a trial and there are instances where it has damaged the long-term capability of the Agencies.

69. Information that would damage national security if it were published is protected through the DA-Notice system (formerly known as the D-Notice system). This provides advice and guidance to the media about defence and counter-terrorism information. Whilst the system is voluntary, has no legal authority, and the final responsibility for deciding whether or not to publish rests solely with the editor or publisher concerned, the system has been effective in the past. However, as the Cabinet Secretary told us, in a changing media climate this was no longer necessarily the case: "*there was a time when the D-Notice operated more effectively [but] I think we have problems now*". Whilst this is very concerning, it does not appear to be irresolvable. The Cabinet Secretary said "*I think we can talk to editors about this*" and we understand that the Agencies are already working with the Defence, Press and Broadcasting Advisory Committee to improve the effectiveness of their relationships with the media.

³⁰ The previous Committee reported on this matter in the 2004–2005 Annual Report, Cm 6510.

70. In the short term, however, the problem is the number of leaks to the media about current operations – both in terms of those who leak sensitive information and those who choose to publish it. The former Director General of the Security Service said of media reporting of the alleged plot to kidnap and murder a British serviceman in February 2007:

We were very angry, but it is not clear who we should be angry with, that most of the story of the arrests in Op GAMBLE were in the media very, very fast. Indeed, before the arrests in Birmingham, the press were pre-positioned and before the police had picked up one of the plotters and the surveillance was still out looking for them, the story was in the press.

So the case was potentially jeopardised by the exposure of what the story was. My officers and the police were jeopardised by them being on operations when the story broke. The strategy of the police for interrogating those arrested was blown out of the water, and my staff felt pretty depressed about the fact that this had happened.³¹

It is very worrying that those who leak these stories and those who publish them can jeopardise counter-terrorism operations, and put lives in danger.

71. Still further problems can arise when the case gets to trial. Some papers have not observed the reporting restrictions in place and, by commenting on matters that are *sub judice*, have caused significant difficulties with the trial.

72. Keeping the public informed about developments is a responsible job that the majority of reporters take very seriously indeed and we commend them for that. However, there are a very small number who, in their desire for a sensationalist headline, forget that this is about people's lives. It is about the lives of officers on operations, and it is about the lives of members of the public. We must not risk a terrorist walking free and launching an attack because his trial was prejudiced by irresponsible media reporting.

M. The Committee believes that the role of the media is more important than ever in the fight against terrorism and that this responsibility must be taken seriously by all concerned. The current system for handling national security information through DA-Notices, and the Agencies' relationships with the media more generally, is not working as effectively as it might and this is putting lives at risk. We recommend that the Government engage with the media to develop a new, effective system, with a view to protecting intelligence work, operations, sources and criminal prosecutions, whilst ensuring that the media continue to report on important matters of public interest.

³¹ Oral evidence – Security Service, 20 March 2007.

THE INTELLIGENCE COMMUNITY

Permanent Secretary, Intelligence, Security and Resilience

73. In its 2005/06 Annual Report, the Committee raised concerns about the dual nature of the role held by the Security and Intelligence Co-ordinator (SIC):

We believe [that a possible conflict of interest] arises from the SIC's responsibility to represent the views and interests of the Intelligence Community to the Prime Minister and the JIC Chairman's responsibility to provide independent, unbiased advice to the Prime Minister.³²

74. In its response to the Committee's 2005–2006 Annual Report, the Government did not accept the Committee's concerns, seeing no conflict between the two roles and describing them as “*mutually reinforcing*”. We returned to this matter with the Cabinet Secretary and the current post-holder, Sir Richard Mottram, this year. In evidence, both acknowledged that the potential for a conflict of interest to arise did exist, but were adamant that the risks were manageable. In August 2006, the SIC post was renamed the Permanent Secretary, Intelligence, Security and Resilience.

75. In late July 2007, however, following a wider review of counter-terrorism arrangements, the Prime Minister announced that the post would be split into the two previous components – the SIC post and the Joint Intelligence Committee (JIC) Chair:

In line with the Butler Report we will separate the position of Chairman of the Joint Intelligence Committee from policy adviser to the Government. And so the sole responsibilities of the Chairman of the Joint Intelligence Committee will be to provide Ministers with assessments which have been formulated independently of the political process and to improve across Government the effectiveness of intelligence analysis.³³

N. Whilst the Committee did not find any evidence of conflict between the roles during the tenure of Sir Richard Mottram, we believe that there would always have been a risk of conflict by virtue of the posts being combined. We are pleased that the Government has decided to revert to the separation of these two important roles.

76. This is a welcome development. We note, however, that the grade of both of these posts will be lower than that of the present combined post and are concerned at the impact this may have on relationships between the holders of these posts and the Heads of Agencies, who are of a higher grade.³⁴ We will monitor this situation.

Joint Intelligence Committee and Assessments Staff

77. During 2006/07, the Assessments Staff has produced approximately 150 papers for the JIC. It has also produced daily intelligence highlights, weekly summaries on key areas

³² Cm 6864, paragraph 9.

³³ Hansard, 25 July 2007, column 841.

³⁴ This represents, in effect, a reversion to the arrangements prior to 2002.

such as Iraq, and other intelligence updates for senior readers around Whitehall. The conflict in the Lebanon required a great deal of work over the summer of 2006, and for a two-month period intelligence analysts were producing daily bulletins on developments to customers in the MoD, the Foreign and Commonwealth Office (FCO), the Cabinet Office, and Number 10. The JIC has also spent a considerable part of 2006 examining other strategic issues, including ***, ***, and the evolving picture of ***.

Professional Head of Intelligence Analysis

78. The Professional Head of Intelligence Analysis (PHIA), Jane Knight, took up her post in September 2005, as part of the Government's implementation of the recommendations of the Butler Review.^{35, 36} The role of the PHIA is to improve co-ordination and best practice in the recruitment, training, methodology and career management of analysts across the intelligence community, and to bridge gaps and remove duplication in analytical capabilities.

79. The Committee took evidence from the PHIA for the first time this year. We were told that the PHIA team has promulgated an analytical competence framework for professional development and is conducting a survey of analytical capabilities across the intelligence community. In terms of training and induction, a number of courses have been developed and introduced to address perceived gaps in training provision, provide analytic methodology and induction courses, and deliver further professional training and best practice.

O. The Committee believes that the Professional Head of Intelligence Analysis is fulfilling an important role in ensuring effective intelligence analysis training and closer working between analysts across the wider intelligence community.

Defence Intelligence Staff

80. The Defence Intelligence Staff (DIS) has been supporting the UK's military operations in Iraq, Afghanistan, and the Balkans during 2006/07, and also supported the UK's non-combatant evacuation operation during the conflict in the Lebanon. Away from these priorities, DIS has maintained effective coverage on areas of global unrest to provide a background intelligence picture to key customers in the MoD and elsewhere. Demand for intelligence on global contingency issues has risen due to a need to provide military planners with advance warning of possible force deployments for security or humanitarian operations.

81. Although DIS does not have direct responsibility for counter-terrorism, its technical expertise on a number of related areas, such as countering proliferation, or improvised explosive devices, has had a direct bearing on Agency counter-terrorism operations. In addition, we have been told that DIS imagery capability – the Joint Air Reconnaissance Intelligence Centre (JARIC) – has provided significant and timely contributions to operations.

³⁵ HC 898.

³⁶ Having completed her two-year posting, the Committee has been informed that Jane Knight retired on 31 August 2007, and her post is currently being filled on a temporary basis by the Deputy PHIA. The identification of a permanent successor has been delayed until the new JIC Chairman (to whom the successor will report) has been appointed.

82. In its 2005–2006 Annual Report, the Committee commented on the modernisation and transformation programme designed to strengthen its ability to address key operational challenges. This has continued during 2006/07. DIS is working to improve its central accommodation arrangements in order to allow better integration with MoD policy and commitment teams, as well as with Ministers and senior defence staff. The modernisation programme has a number of other elements which involve estates rationalisation, integration of collection, communications, sharing and wider dissemination of intelligence. One significant development has been the identification of a new site for JARIC, which will be co-located with the headquarters of the Intelligence Collection Group at Wyton. Separately, DIS is reviewing its training policy and is also awaiting the outcome of further Defence Training Review negotiations on training delivery.

83. Last year, we reported on the recommendations of the Butler Review that had a bearing on DIS. We returned to these matters this year to examine the impact the changes were having on the organisation. DIS appointed a senior civil servant to the post of Professional Head of Defence Intelligence Analysis in summer 2006 to complement the work of the PHIA in the Cabinet Office. This work is further supported by the role of Deputy Chief of Defence Intelligence (DCDI) as “skills champion” for DIS, who is responsible for ensuring that skills and analytical capabilities match future requirements.

84. Following a key recommendation expressed in the Butler Review, we asked DIS about avenues for professional dissent among DIS analysts. The Chief of Defence Intelligence (CDI) confirmed that a process was now in place which allows staff to register professional concerns or matters of conscience in the course of their work to senior MoD management outside of DIS, where it has not been possible to resolve these through the usual line management chain.³⁷ CDI also told the Committee that he recognised the importance of a recommendation from the Butler Review that DCDI should have an intelligence analysis background.³⁸ He said:

it has proved difficult in the past to generate people who can get through the various necessary gates and hurdles to be selected for the Senior Civil Service, then to go on within the Senior Civil Service via a number of appointments, which by necessity implies outwith Defence Intelligence Staff, who can then be selected for the second jump which would be required to fill the post of DCDI.³⁹

CDI explained that DIS has made changes to its personnel, training and development arrangements to provide the opportunity for a future DCDI to have an intelligence analysis background. However, since this relates to staff development and career progression, it will take time to achieve.

³⁷ Butler recommended that the remit of the intelligence and security Agencies’ Staff Counsellor be extended to DIS (HC 898, paragraph 589). The process described by CDI involves the dissent function being undertaken by the MoD’s Personnel Director.

³⁸ HC 898, paragraph 590.

³⁹ Oral evidence – DIS, 1 February 2007.

P. We are satisfied that a process to cater for professional dissent within DIS is now in place and that steps have been taken to improve career development for professional analysts which, in time, will provide access to the most senior appointments within the organisation.

SCOPE

85. SCOPE is a major inter-departmental government IT programme that builds on the intelligence community's existing secure communications network to enable partner agencies and departments in the UK (and key posts overseas) to share information with each other more effectively and improve ways of working. In previous reports, the Committee has expressed its concerns that the programme has experienced delay after delay, that partners were ill prepared for its introduction, and that there were significant risks involved in the new plan of rolling out two significant phases of the programme simultaneously.⁴⁰

86. When we last reported, the programme had provided few measurable benefits and Phase I – developing the SCOPE Service Operations Centre (SOC) and connecting HMRC, SOCA, the Department of Trade and Industry and the Home Office to it – had yet to be achieved.⁴¹ It achieved full operational capability in October 2007 – over two years later than originally forecast (April 2005).

87. Despite this history of delays the programme has maintained the support and commitment of its ten principal stakeholders and we have been told that the wider intelligence community is now finally experiencing the benefits from Phase I. In SOCA, for example, SCOPE forms the backbone to its secure communications and is used to run over *** live operations. The average time taken to initiate and process a “request for information” has been reduced from nearly 12 hours to just 15 minutes by using SCOPE. Another benefit can be seen in improvements to the effectiveness of intelligence: HMRC has reported more fluid and efficient communication and a greater demand for its intelligence as a result. Other departments also report enjoying finally being connected to the secure intelligence network and being able to communicate highly classified information directly and efficiently with the Agencies, FCO, MoD, Cabinet Office and other users.

Q. The Committee welcomes the fact that the SCOPE programme has maintained the support of its stakeholders and that the intelligence community is now experiencing the benefits of being connected to the secure intelligence network.

⁴⁰ Cm 6864, Cm 6510, Cm 6240 and Cm 5837.

⁴¹ The wider intelligence community consists of SOCA, HMRC, the Home Department and the Department for Business, Enterprise and Regulatory Reform (formerly the Department of Trade and Industry).

88. There have been concerns, however, about the SOC. Earlier this year, the Centre suffered a “serious process failure” which resulted in the loss of some operational data. Although an independent review was held immediately after the incident and the conclusions of that review are currently being implemented, we remain concerned at the serious implications of such a failure were it to occur again. A further problem surrounds the staffing of the centre – whilst the SOC is adequately staffed to support Phase I users, there is likely to be a significant challenge to recruit, vet and retain enough highly skilled staff to support the growth in users that will accompany Phase II roll-out (from mid-2008). We note that strategies are in place to address this challenge and also to address succession plans for the head of the SOC, and will monitor how these work.

89. Phase II of the programme – which aims to broaden the user base and enhance existing capability – was scheduled to begin roll-out in June 2007 (it was originally scheduled for the end of 2005). We have been told, however, that despite some aspects of release having been delivered, overall delivery of Phase II has been revised and delayed again (with roll-out between mid-2008 and early 2009) to allow departments to align their business processes and ensure partner readiness.

90. Work also continues on a separate Overseas Project, which aims to deploy SCOPE to *** overseas posts. This project, jointly managed and funded by the FCO and the Central Programme Team, supports secure communications for the FCO and other departments with staff overseas. We have been told that considerable progress has been made with the UK side of the Overseas Project, but that the pilot system, which was scheduled to be installed overseas during the summer, has been delayed because of problems providing a sufficiently secure environment (and the associated costs). The first of the pilot posts will now be installed in December 2007 and the remaining pilots in early 2008.

R. We remain very concerned, however, by the numerous delays to this important programme, including: delays to the delivery of Phase I and Phase II; a general lack of preparedness for full implementation amongst SCOPE partners; and difficulties in providing a secure environment for the deployment of SCOPE overseas.

Serious Organised Crime Agency

91. At the time of our last Annual Report, the Serious Organised Crime Agency (SOCA) had only recently become operational.

92. SOCA faced some significant challenges in its first year, not least how to amalgamate a number of previously independent organisations with different working practices; over 4,000 of SOCA’s staff have joined from its precursor agencies, each of which has had its own modus operandi, and staff terms and conditions, including 43 different pay scales which required consolidation. Staff also had to adapt to a completely novel tasking and prioritisation process. Despite these difficulties, and some inevitable frustrations and teething problems, a survey in December 2006 found that staff were very highly committed to the organisation and its aims.

93. The Committee reported last year that SOCA could face difficulties in recruiting sufficient numbers of staff with the requisite operational, analytical and intelligence assessment skills. SOCA has certainly had no shortage of people applying to join, but has been constrained by budgetary factors. It has therefore placed great emphasis on using existing staff already in the organisation to fit the skills base it needs, though it will take time to develop the depth in skills that is needed.⁴² It is hoped that the merger of the Assets Recovery Agency into SOCA will improve the Agency's expertise in financial investigation.

S. The Serious Organised Crime Agency is a large organisation formed relatively quickly from four separate bodies. It will take some time, in the Committee's view, before its performance can be readily assessed against its strategic aims.

The Commissioners

94. Sir Paul Kennedy, the Interception of Communications Commissioner, and Sir Peter Gibson, the Intelligence Services Commissioner, took up post in April 2006. The new Commissioners have told us that they have been impressed by the integrity and quality of the Agencies' work – particularly by how promptly they report any mistakes.

95. The rise in interception warrant applications in response to increasing counter-terrorism work has levelled off in recent months, and the number of errors in applications or executions has fallen. The Commissioners reported that human sources across the intelligence community were being managed well, and that staff in the Agencies were always conscious of the need for safety and security in agent handling.

Review of counter-terrorism strategy

Context

96. Public expenditure on counter-terrorism and intelligence has risen significantly in recent years. By 2007/08, annual spending on these areas will be £2.5 billion – more than double the level of expenditure before 9/11. The overarching, centrally co-ordinated strategy for counter-terrorism is known as CONTEST.⁴³ It has four key objectives:

- to PREVENT terrorism, by tackling the factors that make individuals, organisations and communities, both in the UK and elsewhere, prone to violent extremism;
- to PURSUE terrorists and those who sponsor their campaigns by disrupting their activities;
- to PROTECT against terrorist attacks on UK citizens, key national services and UK interests abroad; and
- to PREPARE the UK to be as ready as it can be for the consequences of a terrorist attack.

⁴² 1,600 training courses were delivered to SOCA staff last year, with 10,000 attendees.

⁴³ Cm 6888.

97. A review of the CONTEST strategy by the Prime Minister's Delivery Unit was leaked to the media in the autumn of 2005. It was reported to have said that there was:

*little effective coordination and no clear leadership... [There was] little confidence in the ability of the security apparatus to tackle the problem and difficult to demonstrate that progress has been made... [Key policies were] unrelated to the real world and showed no signs of making progress.*⁴⁴

The review is reported to have concluded that: *"the strategy is immature. Forward planning is disjointed or has yet to occur. Accountability for delivery is weak. Real world impact is seldom measured."*⁴⁵

98. In a parliamentary debate on counter-terrorism strategy, the then Home Secretary said:

*We take the lessons of [the review] very seriously, and we are doing everything possible to make sure that we improve our performance at every opportunity.*⁴⁶

99. In the wake of Operation OVERT, the Prime Minister asked the Home Secretary to lead a review of the Government's counter-terrorism policies, approach and structures. The review group included the Foreign Secretary and the Secretary of State for Communities and Local Government, as well as the Agencies and the police.

The rationale for change

100. Giving evidence to the Committee in early March 2007, the then Home Secretary expressed concern at the current counter-terrorism arrangements, and made the case for greater, dedicated political oversight. He based this on what he saw as a mismatch between the threat and the Government's response, saying:

If you look at "threat", which is normally defined by intention and capability, we are facing an enemy with unconstrained intent... who is not bound by any international convention, who respects no legality, and who do not distinguish between combatants and non combatants, between civilians and others, between men, women and children, or between people of any religion... and therefore you truly have an unconstrained intention to murder, massacre and destroy on an unconstrained scale...

*We have to have an integrated response... with political oversight, which in my view has been sadly lacking for the past few years... [and a] delivery department... with strategic functions, [with] the capacity to deal with the central issue, which is a battle for ideals and values. If we do not have that in an integrated fashion, we will not be stepping up [to] the mark.*⁴⁷

⁴⁴ "Labour's war on terror is failing, says leaked report", *The Sunday Times*, 23 October 2005.

⁴⁵ *Ibid.*

⁴⁶ *Hansard*, 10 July 2006, column 1121.

⁴⁷ *Oral evidence – Home Secretary*, 13 March 2007.

The changes

101. The Prime Minister agreed with the Home Secretary's view and on 29 March 2007, as part of wider changes within the Home Office, the Government announced two key changes to improve the counter-terrorism and security capabilities of the Government.⁴⁸ They included:

- a new Ministerial Committee on Security and Terrorism, chaired by the Prime Minister and supported by a number of Sub-Committees; and
- the establishment of an Office for Security and Counter-Terrorism to take on overall responsibility for the CONTEST strategy from the Cabinet Office and carry out horizon-scanning, strategy, planning, and programme management.

T. The Committee has made clear in previous Annual Reports its concern that the Ministerial Committee on the Intelligence Services (CSI) was not used as a forum for ensuring Ministerial co-ordination on intelligence and security issues. We are pleased, therefore, that a new Committee has been established to enable Ministers to meet formally to discuss these issues.

102. On 25 July 2007, the Prime Minister reported to Parliament the changes that the new committee (since named the Ministerial Committee on National Security, International Relations and Development) had recommended. These included the publication of a National Security Strategy, the first of which would be "*published and presented [to Parliament] in the autumn*".⁴⁹ We are currently awaiting an update on these developments.

Official Secrets Act

103. We reported last year that the Home Office had bid for a place in the legislative programme to amend the Official Secrets Act 1989. The former Home Secretary told the Committee: "*We think this is worth doing, we would like to do it... we could not get parliamentary support.*"⁵⁰ The Committee agrees that the Act should be amended and repeats its offer to comment on any draft legislation prior to its introduction.

⁴⁸ *Written Ministerial Statement by the Prime Minister, 29 March 2007.*

⁴⁹ *Hansard, 25 July 2007, column 841.*

⁵⁰ *Oral evidence – Home Secretary, 13 March 2007.*

OTHER ISSUES

Investigation into BAE Systems

104. In December 2006, the Serious Fraud Office (SFO) decided to halt its investigation into allegations of financial irregularities in BAE Systems' dealings with members of the Saudi royal family. The Attorney General said of the decision:

All relevant agencies were clear about the crucial importance of UK-Saudi co-operation in the fight against terrorism and the damage to UK interests – and, potentially, UK lives – if that co-operation were withdrawn. Having been advised of the risk to national security if the SFO investigation continued, the director of the SFO concluded that it was not a risk that could properly be taken in the public interest. I repeat that it was the director's decision, not mine...

The SIS has made it clear publicly that it shares the concerns of others within government over the possible consequences for the public interest of the SFO investigation... Before the SFO decision was taken, I discussed the matter with the head of the SIS, whose view was that the Saudis might withdraw their co-operation if the SFO investigation continued and that they could decide to do so at any time...

Saudi Arabia is a source of valuable streams of intelligence on al-Qaeda and, if Saudi Arabia were to withdraw that co-operation, the UK would be deprived of a key partner in our global counter-terrorism strategy.⁵¹

105. The Committee discussed this matter with Lord Goldsmith, Sir Richard Mottram and the Chief of SIS. We have also seen the classified note, prepared by Sir Richard Mottram, entitled *The Saudi contribution to our domestic and international efforts to combat terrorism*, which was provided to the Attorney General, and shown to the Director of the SFO, under cover of a minute from the Prime Minister.⁵² We asked for sight of this minute – or those parts of it relevant to the intelligence and security relationship – but were refused on the grounds that it was concerned with wider public interest issues.⁵³ Our interest in the matter is limited to the intelligence relationship, not the wider issues, and we have questioned those involved on that basis.

106. We asked the Chief of SIS about the Saudi threat to withdraw co-operation:

*There was some suggestion in some of the media coverage that there was no *** threat to our co-operation... that is not true. There were threats made to the existence of the co-operation [and] there was reason to take those threats seriously...*

Now, if the threats were carried out and if the co-operation in the area of intelligence and security was withdrawn... then the question is: "how valuable is that

⁵¹ Lords Hansard, 18 January 2007, column 778.

⁵² We have been told that Sir Richard's note to the Attorney General was prepared from material provided by the Agencies and from JIC assessments.

⁵³ The Committee has been told that "the Prime Minister's minute was concerned with the wider public interest issues... [It] did no more than draw attention to the key benefits arising from the relationship to the UK's efforts to protect British lives and interests as set out in [Sir Richard Mottram's] note... Beyond that, the Prime Minister simply explained that he had good reason to believe that those benefits were at risk." – letter from the Cabinet Office, 13 November 2007.

co-operation?” The answer is that it is valuable... Saudi Arabia is an absolutely key country... since May 2003, when the first big attacks happened in Riyadh... they have turned themselves into a very important and powerful player in the world counter-terrorism campaign... They have done that very effectively and one of the reasons they are effective is because they co-operate well with the international community, including us. But that equally, is very, very beneficial for us. They are one of the most important countries in this area... And clearly Saudi Arabia is right at the very top of the list of important countries.⁵⁴

107. The SFO confirmed its reasons for halting the investigation. The Director of the SFO told the Committee:

Normally a decision [about whether or not to prosecute] is made only after the evidence has been gathered but in this case it became clear that it was the continuance of the investigation itself and in particular the investigation of the accounts in Switzerland that was likely to cause offence to the Saudi Arabian authorities which would lead to damage to the public interest.

[During] October and November 2006... we received representations that continuing the investigation was likely to cause, and indeed was beginning to cause, serious damage to our relations with Saudi Arabia and thus our cooperation with them in relation to national and international security...

I was satisfied that pursuing the investigation into the Swiss accounts, or indeed attempting to bring any prosecution which involved naming the Saudi Princes, would result in a withdrawal of cooperation including cooperation in respect of security... I came to the view on 13 December 2006 that continuing the investigation would not be in the overall public interest.⁵⁵

U. The Committee is satisfied that, at the time, there were serious national security considerations which contributed to the Serious Fraud Office’s decision to halt the investigation into BAE Systems’ dealings with Saudi Arabia.

⁵⁴ Oral evidence – SIS, 23 January 2007.

⁵⁵ Letter from Robert Wardle, Director of the SFO, 16 October 2007.

Intercept as evidence

108. Current legislation prohibits giving any evidence or doing anything else in connection with a legal action that would disclose or imply the interception of communications by law enforcement or intelligence agencies. This means that intercept material, with certain exceptions, cannot be used in evidence in any criminal proceedings.⁵⁶ In light of certain other counter-terrorism measures adopted by the Government and Parliament – such as extended pre-charge detention and Control Orders – there has been renewed pressure from some quarters to remove the ban on the use of intercept material.

109. The Committee has spoken to the former Home Secretary John Reid, the former Attorney General Lord Goldsmith, the Heads of the Agencies, Sir Richard Mottram, and Lord Carlile (the Government’s Independent Reviewer of Counter-Terrorism Legislation). We have also discussed these issues with the Interception of Communications and Intelligence Services Commissioners.

110. We had hoped to take into account the Home Office study on the effect of changes in technology on interception and its review of Control Orders but, despite repeated requests over the last year, we have only just been provided with these as the Report was being sent to the Prime Minister. We have therefore had no opportunity to consider them. This is an example of how we have been hampered in our ability to do our job this year by a government department failing to provide us with information in sufficient time.

111. The concerns of this Committee have centred on whether or not there is a net benefit, in terms of national security, from introducing intercept into the courts. At its simplest, it is a question of whether using intercept material in court would result in more terrorist convictions than are already achieved through its use to generate leads, and whether these would be sufficient to outweigh the possible reduction in the capability of the Agencies to identify the terrorists and disrupt attacks in the first place.

112. Those in favour of lifting the ban have argued that, logically, the prosecution must be able to take advantage of every piece of evidence it can when trying to secure the conviction of terrorists and serious criminals: if there is intercept that would help their case, then they should be able to use it. They argue that the Government should not be requesting Control Orders to contain terrorist suspects that it cannot successfully prosecute when it is not using all the available evidence. They also argue that the nature of intercept evidence can be instrumental in persuading a defendant to plead guilty or help the prosecution in other ways.

⁵⁶ *The ban on the use of intercept as evidence is established by Section 17 of the Regulation of Investigatory Powers Act (RIPA) 2000. Section 18 of RIPA exempts certain specified legal proceedings from this general prohibition. The prohibition on evidential use applies to material intercepted under an interception warrant or obtained unlawfully. It does not apply to interception which has lawful authority by virtue of the fact that both parties consent, or one party consents and a directed surveillance authorisation is in place or it takes place under lawful business practice regulations. Accordingly, such communications are admissible in evidence (and disclosable). No equivalent prohibition applies to the evidential use of material obtained through surveillance, including eavesdropping, covert closed-circuit television and observations made by covert surveillance officers.*

113. The Agencies, however, are adamant that their intercept capabilities must not be disclosed in court. If they were, criminals and terrorists would quickly learn what the Agencies can and cannot do, and would find means of avoiding detection, which would then damage their capability and coverage. Other countries, however, allow the use of intercept as evidence without any adverse impact on their security and intelligence capability, so what makes the UK different? GCHQ points to a unique combination of factors in the UK:

The UK is the only country which has all three of the following things: an adversarial legal system, subordination to [the European Convention on Human Rights] and a strategic intercept and SIGINT capacity that is worth protecting.⁵⁷

114. In practice, because of the UK's adversarial legal system, the defence would be able to test the validity of evidence and thereby explore how it was obtained. As communications technology evolves (particularly internet protocol), we understand it may be difficult for the Agencies to be able to prove intercept to an evidential standard. In addition, whilst it may be possible to prevent defence probing of the actual technique, we understand that mere revelation of intercepted material could compromise sensitive capabilities: the Agencies, understandably, clearly wish to protect what they can and cannot do.

115. A further argument we have considered is the additional burden that would arise from a requirement to record and retain all intercept material of potential relevance to a future prosecution and, in the event of such a prosecution, to review that material for disclosure purposes.⁵⁸ This would place a huge administrative and resource burden on the Agencies, which we consider they are ill placed to shoulder at a time when they are stretched trying to provide coverage of the terrorist threat to the UK.

116. ***

***.⁵⁹

117. The Director of GCHQ summarised the test for allowing intercept:

... a change to allow intercept as evidence should be introduced only when doing so would have a net benefit in securing the safety and the security of the UK. By that I mean not just convicting and imprisoning criminals, but also preventing crimes and terrorist actions.⁶⁰

⁵⁷ Oral evidence – GCHQ, 8 March 2007. GCHQ also pointed to the closeness of the working relationship between the intelligence and security Agencies and the law enforcement authorities in the UK, which results in a great deal of both detection and prevention of crime, as another fundamental reason for the UK's unique position on intercept.

⁵⁸ Subject to any successful claim to refuse disclosure on Public Interest Immunity grounds.

⁵⁹ Oral evidence – Home Office, 13 March 2007.

⁶⁰ Oral evidence – GCHQ, 8 March 2007.

118. The issue, therefore, is whether permitting intercept as evidence would have a real long-term impact in terms of securing more convictions than already secured by the use of intercept for intelligence leads. Having not been shown the Home Office study on this, we have yet to see any hard evidence.⁶¹ Giving evidence to the Committee, GCHQ summarised its position on lifting the ban on the use of intercept material: “*So far we do not believe that anything proposed passes the test of doing more good than harm, and we are convinced that it would lead to a net reduction in our national ability to deal with crime and terrorism.*”⁶²

119. The Home Secretary shared these concerns: “*There would be benefits in an ideal world. But I do not believe you could do this without a huge risk of a downside for our operational capacity in the long term, and I am very wary of winning the minutes but losing the hours.*”⁶³

V. Intercept is of crucial importance to the capability of the Agencies to protect the UK, its citizens and its interests overseas. Any move to permit the use of intercept evidence in court proceedings must be on a basis that does not jeopardise that capability.

120. Whilst we have examined whether or not intercept should be admitted as evidence insofar as it relates to the work of the intelligence and security Agencies, we note that the Prime Minister has established a cross-party Privy Council review of the wider issue. The review is being led by the Rt. Hon. Sir John Chilcott and includes the Rt. Hon. Alan Beith, MP, a member of this Committee. We have submitted our findings to this review.

⁶¹ See paragraph 110.

⁶² Oral evidence – GCHQ, 8 March 2007.

⁶³ Oral evidence – Home Office, 13 March 2007.

ANNEX A – REFORM OF THE ISC

The Governance of Britain *Green Paper*

121. The following is an extract on the ISC from the Government's Green Paper on constitutional reform:⁶⁴

Intelligence and Security Committee

89. *Ensuring the security of the nation in the face of terrorist and other dangers is the first responsibility of government. The security and intelligence Agencies play a vital role in this and other aspects of the Government's national security policies. To ensure that these Agencies command full public support for, and confidence in, the work they do it is important that the representatives of the people hold them to account in an appropriate manner, while respecting operational sensitivities.*

90. *The work of the security and intelligence Agencies often, by its nature, involves highly-classified information, disclosure of which would be gravely damaging to the national interest and could put individuals at risk. This must be a fundamental consideration in determining the conduct of parliamentary scrutiny if the oversight is not to undermine the operational effectiveness of the Agencies. In order to exercise effective oversight over the expenditure, administration and policy of the Agencies, the Committee scrutinising their work needs regular access to much more highly-classified information and evidence than that normally shared with select committees of the House. The Intelligence and Security Committee (ISC) was, therefore, established – as, effectively, the Select Committee for the Agencies – under separate legislation by the Intelligence Services Act 1994.*

91. *The ISC has senior and well-qualified membership from both Houses, drawn from all the major parties. It has acted independently and assiduously to scrutinise the work of the Agencies and other parts of the intelligence community. Its reports are published and debated in Parliament. However, because they are prepared under separate arrangements and the Committee meets only in private, some argue that the process is insufficiently transparent.*

92. *So the Government proposes to consult on how the statutory basis of the Intelligence and Security Committee should be amended to bring the way in which it is appointed, operates and reports as far as possible into line with that of other select committees, while maintaining the necessary arrangements for access to, and safeguarding of, highly-classified information on which effective security depends.*

⁶⁴ Cm 7170.

93. *While the consultation on the Committee's statutory basis is ongoing, a number of interim changes could be made within the existing legislation:*

- *greater transparency over how Committee members are appointed, using similar processes of consultation between the major parties as those for select committee selection;*
- *giving the Committee the option to meet in public (including, if Parliament agrees, in the Houses of Parliament);*
- *House of Commons debates on the Committee's reports, to be led by the Chair of the Committee rather than by a Government Minister, with reports also debated in the House of Lords; and*
- *strengthening the Secretariat to the Committee, including through the appointment of an independent investigator, and making the Secretariat clearly separate from the staff of the Cabinet Office. (The Committee takes evidence in, and has a Secretariat based in, the Cabinet Office for security reasons).*

94. *There is also an overlapping agenda between the work of the Home Affairs Committee, the Foreign Affairs Select Committee and the ISC with all three touching on issues relating to counter-terrorism and security. The Government is keen that their oversight activity is, taken together, as effective as possible.*

95. *The Government will invite the Chair of the Committee to advise on how to maximise the effectiveness of the Committee's scrutiny role, including on the Committee's relationship to Parliament and to relevant select committees, under the existing legislation.*

96. *Following consultation, the Government will then bring forward proposals to take the reforms further on a revised statutory basis.*

National Security Strategy

97. *The Government will publish a National Security Strategy setting out our approach to the range of security challenges and opportunities we face, now and in the future and both at home and overseas. The strategy will set the framework for taking forward those issues across a range of departments and agencies, and provide the basis for deciding on changes in priorities to reflect changed circumstances.*

98. *To oversee the development and delivery of that strategy, and the Government's wider international, European and international development policies, the Government will establish a National Security Committee to ensure that its policies and their delivery are coordinated and appropriate to the changing nature of the risks and challenges facing us in the 21st century. The Committee will meet regularly, under the Chairmanship of the Prime Minister, and comprise senior Cabinet colleagues from relevant departments, supported by relevant senior officials and a secretariat in the Cabinet Office. It will replace the existing Ministerial Committees on Defence and Overseas Policy, Security and Terrorism, and Europe.*

Parliamentary debate

122. The Prime Minister's statement to the House on 3 July 2007 introduced *The Governance of Britain Green Paper*. The following are extracts from that statement and the debate which followed:

*The Prime Minister: As the security agencies themselves recognise, greater accountability to Parliament can strengthen still further public support for the work that they do. So while ensuring necessary safeguards that respect confidentiality and security, we will now consult on whether and how the Intelligence and Security Committee can be appointed by, and report to, Parliament. And we will start now with hearings, held in public wherever possible; a strengthened capacity for investigations; reports subject to more parliamentary debate; and greater transparency over appointments to the Committee.*⁶⁵

Mr Paul Murphy: I congratulate my right hon. Friend on a most remarkable document [The Governance of Britain Green Paper], but more particularly I welcome the proposals that he has put before the House on ensuring that the Intelligence and Security Committee, which I chair, will be more transparent and accountable. May I reassure him that all members of the Committee, from whatever party, look forward to examining the proposals to make the Committee more transparent, and particularly the proposals on holding more debates in this Chamber and the Chamber of the other place?

*The Prime Minister: I am grateful to my right hon. Friend, who has been an excellent chairman of the Intelligence and Security Committee. He had led the way in suggesting that reforms can be made. I feel that the two functions of a Select Committee are first, to investigate, to interrogate and to examine events and what is happening in our country, and secondly, to persuade the country that important things are being done by the services that the Committees are monitoring. It is the second function to which we can now turn our attention. If we have a national security strategy, and if there is a debate on that both in Parliament and in the country, and if there is a power to call witnesses and to report on that, I believe that that second important job of a Select Committee, which is to inform the country of the good work that our services are doing, can be best achieved. I hope that my right hon. Friend will be able to take forward the proposals.*⁶⁶

⁶⁵ Hansard, 3 July 2007, column 817.

⁶⁶ Hansard, 3 July 2007, column 825.

ANNEX B – ACCESS TO PAPERS

123. In ***, the former Intelligence and Security Committee took evidence on a matter. The Committee was given categorical assurances as to what had happened, but nevertheless felt it necessary to have sight of the relevant ministerial submission.

124. A request for sight of the submission was refused by the then Foreign Secretary (***) who said that he himself could not see the papers since they related to a previous administration. When the Committee approached the Foreign Secretary to whom the original submission was made (***), he confirmed that he had no objection to either the serving Foreign Secretary or the Committee seeing the document in question. However, subsequent approaches to the Cabinet Secretary, the Foreign Secretary, and the Prime Minister still resulted in a refusal.

125. The primary reason for this refusal has been that the Committee was told all the relevant information from the submission and therefore has no need to see the actual document. Additional reasons cited have been: that the police were conducting an investigation (the following year);⁶⁷ that the submission would be outside the remit of the Committee (later the same year); and that the papers remain sensitive as defined in Schedule 3 of the Intelligence Services Act and there is no public interest argument for the Committee to see the papers (four years after the original request for the papers).

126. At this Committee's meeting with the Prime Minister in July 2006, we were told that the matter would be reviewed once again, although this instruction does not appear to have filtered down to those concerned.

W. It is now over * years since the Intelligence and Security Committee first requested access to the relevant documentation on this important matter. The Committee notes that this is the only issue on which the Government has refused a Committee request for documents. Given the Prime Minister's expressed intention to strengthen the Committee, such refusal to grant access to documents relevant to our enquiries makes that position untenable.**

⁶⁷ *The Committee has been told that the police found no cause to take further action as a result of this investigation.*

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

A. We would like to record our thanks and praise to the staff of the intelligence and security Agencies, as well as the police and our overseas partners, for all their hard work.

B. We are concerned that aspects of key intelligence and security work are suffering as a consequence of the focus on counter-terrorism priorities. We believe consideration may need to be given to separate, additional funding to maintain the Agencies' capabilities in these areas.

C. We wish to note that whilst the Agencies themselves handle the Committee's requests for information promptly, our work this year has been hampered on occasion by government departments failing to keep the Committee formally informed of changes relevant to its work.

D. We welcome the increase in the Single Intelligence Account for the next three years: it responds to the increased scale of the threat, and the growth of the work needed by the Agencies to counter it. The Committee intends, in the coming year, to investigate the allocation of the increased CSR07 settlement between the three Agencies and the associated spending plans.

E. The Committee is reassured that the Security Service is managing to minimise the risk that inevitably accompanies a rapid growth in staff numbers.

F. The Committee has been impressed by the speed at which the regionalisation programme has been carried out and the clear benefits it has brought.

G. Payments from public funds, including payments to agents, must be properly managed and recorded. We are pleased that steps have been taken by SIS to correct this problem and will monitor compliance and accuracy levels in the future.

H. We conclude that there has been a lack of progress regarding the business continuity of SIS system back-ups. We also note that issues surrounding SIS's retirement age and pensions policy appear to have not yet been resolved. The Committee recommends that these matters are now given a greater priority.

I. The substantial growth in the number of Security Service counter-terrorism operations in recent years has made it difficult for GCHQ to maintain high-quality support to an ever-growing number of investigations. We will monitor the impact of the CSR07 settlement on resolving this problem.

J. The Committee is satisfied that, despite the substantial costs involved, the current SIGINT Modernisation programme represents an essential investment in maintaining GCHQ's technological capabilities. Given the unremitting progress of technology – particularly internet-based communications – we believe it is vital that plans and budgets

are established early to ensure that GCHQ is able to continue vital modernisation work. The Committee will continue to monitor the existing programme and intends to study these future plans carefully.

K. We conclude that, in the circumstances, GCHQ has handled its accommodation problem effectively and achieved the best value for money for the taxpayer in the short term.

L. We are very concerned that, had the flooding continued for very much longer or been more severe, GCHQ's operations could have been even more severely disrupted. In light of these events, the Committee intends to undertake a review of business continuity arrangements for all three Agencies in the coming year.

M. The Committee believes that the role of the media is more important than ever in the fight against terrorism and that this responsibility must be taken seriously by all concerned. The current system for handling national security information through DA-Notices, and the Agencies' relationships with the media more generally, is not working as effectively as it might and this is putting lives at risk. We recommend that the Government engage with the media to develop a new, effective system, with a view to protecting intelligence work, operations, sources and criminal prosecutions, whilst ensuring that the media continue to report on important matters of public interest.

N. Whilst the Committee did not find any evidence of conflict between the roles during the tenure of Sir Richard Mottram, we believe that there would always have been a risk of conflict by virtue of the posts being combined. We are pleased that the Government has decided to revert to the separation of these two important roles.

O. The Committee believes that the Professional Head of Intelligence Analysis is fulfilling an important role in ensuring effective intelligence analysis training and closer working between analysts across the wider intelligence community.

P. We are satisfied that a process to cater for professional dissent within DIS is now in place and that steps have been taken to improve career development for professional analysts which, in time, will provide access to the most senior appointments within the organisation.

Q. The Committee welcomes the fact that the SCOPE programme has maintained the support of its stakeholders and that the intelligence community is now experiencing the benefits of being connected to the secure intelligence network.

R. We remain very concerned, however, by the numerous delays to this important programme, including: delays to the delivery of Phase I and Phase II; a general lack of preparedness for full implementation amongst SCOPE partners; and difficulties in providing a secure environment for the deployment of SCOPE overseas.

S. The Serious Organised Crime Agency is a large organisation formed relatively quickly from four separate bodies. It will take some time, in the Committee's view, before its performance can be readily assessed against its strategic aims.

T. The Committee has made clear in previous Annual Reports its concern that the Ministerial Committee on the Intelligence Services (CSI) was not used as a forum for ensuring Ministerial co-ordination on intelligence and security issues. We are pleased, therefore, that a new Committee has been established to enable Ministers to meet formally to discuss these issues.

U. The Committee is satisfied that, at the time, there were serious national security considerations which contributed to the Serious Fraud Office's decision to halt the investigation into BAE Systems' dealings with Saudi Arabia.

V. Intercept is of crucial importance to the capability of the Agencies to protect the UK, its citizens and its interests overseas. Any move to permit the use of intercept evidence in court proceedings must be on a basis that does not jeopardise that capability.

W. It is now over *** years since the Intelligence and Security Committee first requested access to the relevant documentation on this important matter. The Committee notes that this is the only issue on which the Government has refused a Committee request for documents. Given the Prime Minister's expressed intention to strengthen the Committee, such refusal to grant access to documents relevant to our enquiries makes that position untenable.

LIST OF WITNESSES

Ministers

The Rt. Hon. John Reid, MP – Home Secretary (until 27 June 2007)

Lord Goldsmith, PC QC – Attorney General (until 27 June 2007)

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Sir David Pepper KCMG – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Scarlett CMG – Chief, SIS

Other officials

SECURITY SERVICE

Dame Eliza Manningham-Buller DCB – Director General, Security Service

(until 20 April 2007)

Mr Jonathan Evans – Director General, Security Service (from 21 April 2007)

Other officials

CABINET OFFICE

Sir Gus O'Donnell KCB – Cabinet Secretary

Sir Richard Mottram GCB – Permanent Secretary, Security, Intelligence and Resilience

Mr Chris Wright – Director, Security and Intelligence

Mr Tim Dowse – Chief of the Assessments Staff

Dr Michael Taylor – SCOPE Programme Director

Ms Jane Knight – Professional Head of Intelligence Analysis

Other officials

MINISTRY OF DEFENCE

Air Marshal Stuart Peach – Chief of Defence Intelligence

SERIOUS ORGANISED CRIME AGENCY

Sir Stephen Lander – Chairman, SOCA

Mr Bill Hughes – Director General, SOCA

OTHER

Lord Carlile of Berriew QC – Independent Reviewer of Counter-Terrorism Legislation



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

TSO Shops

16 Arthur Street, Belfast BT1 4GD

028 9023 8451 Fax 028 9023 5401

71 Lothian Road, Edinburgh EH3 9AZ

0870 606 5566 Fax 0870 606 5588

The Parliamentary Bookshop

12 Bridge Street, Parliament Square,

London SW1A 2JX

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-172992-5



9 780101 729925