Intelligence and Security Committee

Annual Report 2011–2012

Chairman:

The Rt. Hon. Sir Malcolm Rifkind, MP

Intelligence and Security Committee – Annual Report 2011–2012

TSO

TSO
information & publishing solutions

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

Online
www.tsoshop.co.uk

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

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

TSO@Blackwell and other accredited agents

ISBN 978-0-10-184032-3

9 780101 840323

Intelligence and Security Committee

Annual Report 2011–2012

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

Intelligence Services Act 1994
Chapter 13

Presented to Parliament by the Prime Minister
By Command of Her Majesty
July 2012

Cm 8403 £21.25

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

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

ISBN: 9780101840323

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

ID P002500979 07/12 21937 19585

Printed on paper containing 75% recycled fibre content minimum.

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

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

ISC 4.20/004 28 June 2012

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

Dear Prime Minister,

I enclose the Intelligence and Security Committee's (ISC's) Annual Report for 2011–2012. This Report details the work and conclusions of the ISC for the period from June 2011 to June 2012.

The Committee has held 28 formal sessions during this period. The majority of the Committee's time was spent examining and taking evidence on the work of the three intelligence and security Agencies and the wider intelligence community. We report on these matters here. In addition to this work, the Committee has been conducting a number of other Inquiries this year: we will conclude these and report accordingly during the next session.

Last year, the Committee put forward proposals to strengthen the independent oversight of the intelligence community, and these are reflected in the Justice and Security Bill currently before the Lords. Once the Bill is enacted, the ISC will have become a statutory Committee of Parliament independent of Government. It will have important new powers to obtain information from the intelligence and security Agencies and will provide proper oversight of their activities, including operations.

Yours sincerely,

MALCOLM RIFKIND

THE INTELLIGENCE AND SECURITY COMMITTEE

The Rt. Hon. Sir Malcolm Rifkind, MP (Chairman)

The Rt. Hon. Hazel Blears, MP
The Rt. Hon. Lord Butler KG GCB CVO
The Rt. Hon. Sir Menzies Campbell CBE QC, MP
Mr Mark Field, MP
The Rt. Hon. Paul Goggins, MP
The Rt. Hon. George Howarth, MP
Dr Julian Lewis, MP
Lord Lothian QC PC

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

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

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

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

The Prime Minister publishes the Committee's reports: the public versions have sensitive material that would damage national security blanked out ('redacted'). This is indicated by *** in the text. The intelligence and security Agencies may request the redaction of sensitive material in the Report which would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee considers these requests for redaction in considerable detail. The Agencies have to demonstrate clearly how publication of the material in question would be damaging before the Committee agrees to redact it. The Committee aims to ensure that only the bare minimum of text is redacted from the Report. We also believe that it is important that Parliament and the public should be able to see where we have had to redact information, rather than keeping this secret. Under the existing legislation the Prime Minister has the power to redact material without the Committee's consent, making a statement to that effect when he lays the Report before Parliament. To date, this has never happened.

CONTENTS

THE WORK OF THE COMMITTEE

1. This Report details the work and conclusions of the Intelligence and Security Committee (ISC) for the period from June 2011 to June 2012. The Committee has held 28 formal sessions and 16 other meetings during this period.

2. The majority of the Committee's time during the reporting period was spent examining and taking evidence on the work of the three intelligence and security Agencies and the wider intelligence community. We report on these matters here. This year's Report takes a more thematic approach, which reflects the close working between the Agencies on many of these issues. In addition to this Annual Report, we have, during the course of the year, written separately to the Prime Minister on two specific issues.

3. We have also continued our work on reform of this Committee in order to provide greater openness and transparency, and reassurance to the public and Parliament that our intelligence and security Agencies are held to account. Last year we provided proposals to the Prime Minister and these were reflected in the Government's Justice and Security Green Paper, published in October 2011. On 28 May 2012, the Justice and Security Bill was introduced to Parliament.

4. In addition to our evidence sessions with the three Agencies, we have also taken evidence from Defence Intelligence, the Joint Intelligence Committee (JIC) and the National Security Adviser, as well as the Foreign Secretary and the Home Secretary. We also held an informal session with the Interception of Communications Commissioner, the Intelligence Services Commissioner and the President of the Investigatory Powers Tribunal to discuss their work over the last year. The Committee has visited all three intelligence and security Agencies and Defence Intelligence in the Ministry of Defence. We have held bilateral discussions with politicians and key officials in Canada, Israel, the Palestinian Authority and the US and hosted parliamentarians and officials from Canada, India, Iraq and Israel. Members of the Committee have also contributed to a number of intelligence-related seminars and conferences in the UK and more widely.

5. The ISC continues to be supported by a small Secretariat comprising personnel from the Civil Service and Parliament. Our Secretariat operates independently of Government and is responsible to the Committee. We wish to record our deep thanks for their hard work and dedication over the year.

KEY THEMES

6. The key themes that have emerged from our scrutiny of the UK intelligence community this year are presented below. Whilst we are critical in some areas where we have uncovered problems, this must not detract from our overall conclusion: it is the hard work and professionalism of those who work in the Security Service, SIS, GCHQ and Defence Intelligence (DI) that kept the UK – and in some cases our allies too – safe during 2011–12. We continue to be impressed by their dedication and effectiveness.

Justice and Security Bill

7. In October 2011 the Government published its Justice and Security Green Paper. This outlined proposals to strengthen the oversight of the intelligence community as well as planned reforms concerning the handling of sensitive material in civil proceedings. Following a period of consultation, the Government subsequently published the Justice and Security Bill on 28 May 2012.

8. The Bill proposes the major reform of the powers of the Intelligence and Security Committee in line with the recommendations made by the Committee itself. It broadens the remit of the Committee to include oversight of the whole of the UK intelligence community as well as retrospective oversight of operational matters, where it is in the national interest and not detrimental to national security. It also removes the right of Agency Heads to withhold information from the Committee (although we are not aware of any instances where they have done so), instead allowing only the relevant Secretary of State a right of veto where appropriate for reasons of national security. There remains further work to be done to produce a Memorandum of Understanding which will set out the procedures that the Agencies will follow in responding to the requirements of the Committee, and to secure the additional staff and researchers necessary to fulfil this expanded remit.

9. The second part of the Bill introduces procedures to protect the most sensitive material in civil cases through the introduction of closed material procedures for those parts of proceedings where national security is at risk. Any exception to the UK's long-standing tradition of open justice is not to be taken lightly. However, at present such cases often do not receive any justice at all, since the cases may have to be abandoned or settled unjustifiably in order not to jeopardise the material in question. What is key is the scope of the material that is to be protected in this way. This Committee has argued strongly that any special arrangements must be the exception, not the rule, and that there were only two very narrow categories of material that should fall to be protected. We therefore welcomed the proposals in the Bill which were far more tightly drawn than those of the Green Paper and address the real issue of protecting only the most sensitive UK intelligence material, and material which has been provided by another country on the strict promise of confidentiality.

Strategic direction and the 'Arab Spring'

10. Last year this Committee welcomed the establishment of the National Security Council (NSC) as a forum for regular discussion of national security matters at the highest level within Government. We have noted this year that the NSC has increased further its status and priority and are pleased to see that the central intelligence machinery and

structures are now better aligned underneath it. This should now provide more coherent strategic direction and clearer tasking of the Agencies.

11. Nevertheless, the real test of the system is how the intelligence community responds to the unexpected. The 'Arab Spring' caught many by surprise and it presented a real challenge to the intelligence community who had to reprioritise quickly and redirect their resources toward the region. We appreciate that it is often impossible to predict such events. However, there does remain a question as to whether, once events began to unfold, the Agencies should have anticipated the possibility that the unrest would spread quickly across the region. This demonstrates the risks that come with drawing down effort completely on lower priority areas: it is important that the Agencies (working with allies where necessary) maintain global intelligence coverage, in addition to the specific priorities set by the NSC. Nevertheless, overall we commend the Agencies for responding well to a fast-moving situation and for their very significant contribution to the UK response.

Counter-Terrorism

12. Al-Qaeda and its affiliates continue to pose a threat to the UK. This year, given the weakened capability of Al-Qaeda Core in Afghanistan and the tribal regions of Pakistan, there has been an increased focus on the growing threat from affiliate groups in the Arabian Peninsula and Somalia. Although Al-Qaeda in the Arabian Peninsula has been weakened by drone strikes targeting its leadership in Yemen, it is a resilient group that is capable of mounting an attack on the West. Nevertheless, the Agencies have continued to see notable successes in their Counter-Terrorism work, even in this testing environment.

13. The ability to place restrictions on individuals who are assessed as posing a terrorist threat but who cannot be prosecuted owing to insufficient evidence that can be disclosed is crucial. In January 2012, the system of Control Orders was replaced by Terrorism Prevention and Investigation Measures (TPIMs). This was accompanied by extra funding for the Security Service and police to help them to manage the additional risk associated with TPIMs. The Committee remains concerned, however, about the potential increase in overall risk as a result of the introduction of the TPIMs regime.

14. While the threat level for Northern Ireland-related terrorism remains SEVERE in Northern Ireland (and SUBSTANTIAL for the rest of the UK), the Security Service considers there to be signs for cautious optimism, with the number of attacks on national security targets falling in 2011. This follows concerted efforts by the Service and police in Northern Ireland, leading to over 200 arrests. This has led in turn to some high-profile convictions, although other cases have resulted in acquittals. Following increases in previous years, the Service intends to maintain its Northern Ireland-related terrorism resources at current levels.

The Olympic and Paralympic Games

15. A continuing theme this year has been the intense work by the intelligence and security Agencies – particularly the Security Service – and law enforcement bodies on security preparations for the Olympic and Paralympic Games to be held in a few weeks' time. This represents a critical security challenge for all concerned. The Security Service has reprioritised its work to enable it to counter any potential threats from Al-Qaeda and its affiliates; republican dissidents; hostile states; and others in the run-up to or during the

Games. This, combined with the burden of the accreditation process and the need to brief and liaise with foreign partners, has placed the Service under unprecedented pressure over the past year and we wish to highlight the exceptional effort made by the staff of all three Agencies during this time.

Cyber security

16. The Committee has previously welcomed the Government's acknowledgement that cyber attacks represent a Tier One risk to the UK. In October 2010, the Government set out its plan to transform the UK's cyber security skills and capabilities by 2015 through the National Cyber Security Programme (NCSP) and accordingly allocated additional funding to the Agencies and other government departments. The Committee has therefore been keen to ascertain what specific outcomes have been achieved thus far.

17. In terms of defensive capabilities, it is clear that the provision of security advice to Government, businesses and individuals will generate the greatest improvement in UK cyber security. Although the Communications-Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI), among others, continue to provide an invaluable service in this regard, we believe that education and basic security measures should be given greater priority in the NCSP. Given the importance of CESG's work in this area we are disappointed that, despite our recommendation last year, a longer-term funding model has still not been established.

18. We note that GCHQ and the other Agencies have made some progress in developing cyber capabilities. However, the Committee is concerned at the lack of progress since the publication of the NCSP: more needs to be done if we are to keep ahead in this fast-paced field.

Counter-Proliferation

19. The UK continues to contribute to international efforts to prevent the proliferation of nuclear weapons. Of particular concern to the UK and our international partners is the prospect of Iran acquiring such weapons. The Committee supports the Government's continuing efforts to apply diplomatic and economic pressure to persuade the Iranian regime to alter its course and we expect the intelligence and security Agencies to be fully involved in these efforts.

Expenditure

20. Last year we reported on the flat-cash settlement that the Agencies received in the 2010 Spending Review (SR10) and the possible impact it may have on their ability to maintain their levels of coverage. We are reassured that a combination of public sector pay constraints and the Agencies' efforts to control other costs has allowed them to maintain their current capabilities. However, the settlement is predicated on all the Agencies making very significant efficiency savings. We have not yet seen firm evidence that these efficiencies will be achieved, particularly those which relate to collaborative working. We therefore recommend that the National Security Adviser immediately seeks to re-evaluate the plans for these savings and assess their viability.

THREAT OVERVIEW

21. The threat to the United Kingdom and its interests overseas continues to come from a number of different sources including: international and Northern Ireland-related terrorism; cyber attacks; Hostile Foreign Activity; and nuclear proliferation. The three intelligence and security Agencies work with the wider intelligence community to counter these threats.

The Olympic and Paralympic Games

- Security preparations for the Olympic and Paralympic Games, which are due to take place in the coming weeks, have been a key challenge over the last year.
- The Agencies and law enforcement bodies have been preparing to counter any potential threats from Al-Qaeda and its affiliates planning an attack in the run-up to, during, or even on the Games; republican terrorist groups planning an attack or a hoax to cause disruption; hostile states increasing their espionage efforts; and possible disruption from unlawful protests or demonstrations during the Games.

International terrorism

- In July 2011, the Joint Terrorism Analysis Centre (JTAC) lowered the threat level from international terrorism in the UK from SEVERE to SUBSTANTIAL.
- Al-Qaeda and its affiliates continue to pose a threat to the United Kingdom. The Al-Qaeda threat has traditionally emanated from Afghanistan and the tribal areas of Pakistan. Although a series of US drone strikes targeting the senior leadership of Al-Qaeda Core in Afghanistan and the tribal areas of Pakistan has weakened their capability to carry out attacks on the West, the threat remains acute.
- The growing threat from Al-Qaeda affiliates has led to an increased focus on the Arabian Peninsula and Somalia. Al-Qaeda in the Arabian Peninsula (AQAP) has maintained a strong presence in Yemen and this has led to an increase in the number of US drone strikes in the region. The death of the radical preacher Anwar Al-Awlaki in September 2011, and of other AQAP leaders since, damaged and, in the short term, reduced the immediacy of the threat from Yemen. However, AQAP has shown itself to be resilient and it remains capable of mounting terrorist attacks against the West. In Somalia, military incursions by Kenyan and Ethiopian forces have resulted in an increase in Al-Shabaab's regional focus. There remains a small contingent of UK citizens fighting for Al-Shabaab, although some of these identify more with the Al-Qaeda cause. The main threat to the UK from Somalia comes from these foreign fighters.
- The terrorist threat in the UK increasingly features attack planning by 'self-starting' or 'home-grown' UK-based groups, who may have been inspired by Al-Qaeda ideology, but not tasked by them. Lone actors – those who have no substantive links to terrorist groups – also continue to pose a risk.

Northern Ireland-related terrorism

- The threat of Northern Ireland-related terrorism remains at SEVERE in Northern Ireland and at SUBSTANTIAL in Great Britain.
- As we noted in last year's Annual Report, this threat comes primarily from republican terrorist groups that have not signed up to the Good Friday Agreement and aim to destabilise Northern Ireland.
- Most attacks in the last year were on the Police Service of Northern Ireland (including the murder of Constable Ronan Kerr on 2 April 2011) but non-security force targets such as banks have also been targeted, with the intention of disrupting normality and generating publicity.

Cyber security

- Cyber attacks continue to be a Tier One threat to the UK.[1] Individuals may be victims of cyber crime; other nation states – in particular China and Russia – may conduct espionage against UK businesses and government; and terrorists may exploit the new opportunities that cyberspace provides to further their aims.

Hostile Foreign Activity

- Government, defence and security interests, as well as the commercial sector, continue to be at risk from traditional espionage by several countries that are targeting UK interests.

Nuclear proliferation

- If Iran were to acquire nuclear weapons technology, other states may feel under pressure to follow. This would lead to instability, particularly in the Middle East, and threaten global security. The UK is engaged in international efforts to prevent nuclear proliferation in the Middle East, with a particular focus on Iran.

[1] *The National Security Strategy sets out the 15 priority risks facing the UK, which are grouped into three Tiers, with Tier One being the highest priority.*

STRATEGIC DIRECTION

National Security Council

22. In our Annual Report last year, we welcomed the establishment of the National Security Council (NSC).[2] The NSC is the main forum for collective discussion of the Government's national security objectives and ensures that Ministers consider national security in a strategic way. We have taken further evidence this year regarding the operation of the NSC to assess the impact its creation has had on the intelligence community. It is evident to us that the NSC has increased further its status and priority, and we are reassured that the requirements of the NSC have been assimilated by the intelligence community.

23. The NSC also has four sub-committees:

Sub-committee	Chair	Terms of Reference	Frequency of meetings
NSC (Afghanistan)	Prime Minister	To consider the implementation of UK Government strategy on Afghanistan to 2014.	Scheduled to meet monthly.
NSC (Threats, Hazards, Resilience and Contingencies)	Prime Minister	To consider issues relating to terrorism and other security threats, hazards, resilience and intelligence policy and the performance and resources of the intelligence and security Agencies.	Meets when required.
NSC (Nuclear)	Prime Minister	To consider issues relating to nuclear deterrence and security.	Scheduled to meet throughout the year.
NSC (Emerging Powers)	Foreign Secretary	To consider matters relating to the UK's relationship with emerging international powers.	Scheduled to meet approximately every 6–8 weeks.

Between 20 March 2011 and 25 October 2011, there was also a sub-committee on Libya, which met, on average, twice a week.

24. We have previously heard from the Agencies that they welcome the greater exposure to Ministers from attending the NSC. This year, Defence Intelligence (DI) has also benefited from this through its involvement in the Libya sub-committee. The Deputy Chief of Defence Intelligence told us: "*As a consequence of our involvement there is*

[2] *The NSC continues to meet weekly, under the chairmanship of the Prime Minister. It is attended by the Deputy Prime Minister; Secretary of State for Foreign and Commonwealth Affairs; Chancellor of the Exchequer, Secretary of State for the Home Department; Secretary of State for Defence; Secretary of State for Energy and Climate Change; Secretary of State for International Development; Chief Secretary to the Treasury; and Minister of State for the Cabinet Office. Others may be invited to attend on occasion.*

more direct tasking from the Prime Minister, from the NSC and others, other key decision makers, the JIC, and our profile, I think, has risen as a consequence of that."[3]

Ministerial tasking

25. The NSC approves the National Security Strategy (NSS) which sets out the 15 priority risks facing the UK and is intended to set the strategic direction for the intelligence community. In addition to the NSS, further direction is given in the Strategic Defence and Security Review (SDSR); the Joint Intelligence Committee's (JIC's) Strategic Priorities for Secret Intelligence Coverage; and the Agencies' own Agency Strategic Objectives (ASOs).

26. The Home and Foreign Secretaries both sit on the NSC, and are each accountable for, and have a close working day-to-day relationship with, the Agencies. We questioned both Secretaries of State as to the extent to which they directed their respective Agencies, and how that related to the other four tasking mechanisms. The Foreign Secretary said:

> *We task them all the time and I discuss with [the Chief of SIS] and with the director of GCHQ on an almost continuous basis their work. So I think, you know, how they allocate their resources is very much guided by us in the Foreign Office. I would say it's set by us predominantly, the overall oversight of these Agencies and their overall strategy is set by us.*[4]

27. The Home Secretary made clear that the relationship with the Security Service is quite different. The Service has a very clear mandate, as set out in the Security Service Act 1989, to protect national security against threats from espionage, terrorism and sabotage. The Act also makes clear that the operations of the Service are under the control of the Director General. The view of successive governments has been that the Security Service should be free from political direction. There is, therefore, less scope for reprioritising at a strategic level – whether by the Home Secretary or the NSC. The Home Secretary explained:

> *I think it is important that there is an operational independence… but there is a process of discussion. I mean, the weekly discussions that I have with the Security Service are about where they are focusing their resources and particular operations that require that resource and questions I can ask about the issues that I see that need to be addressed and how they are doing them. So it's a different sort of accountability.*[5]

28. This difference also translates to the system of Ministerial authorisations. Whilst the Home Secretary issues warrants authorising the Security Service's use of intrusive powers, operational decision-making lies with the Director General who acts, within statutory constraints, in an autonomous fashion (much like the Chief Constable of a police service). On the other hand, the Foreign Secretary is more closely involved in the operational decisions and tasking of SIS and GCHQ: this reflects the greater political and diplomatic risks associated with their overseas operations.

---

[3] *Oral Evidence – Defence Intelligence, 8 March 2012.*
[4] *Oral Evidence – Foreign Secretary, 26 January 2012.*
[5] *Oral Evidence – Home Secretary, 19 January 2012.*

Joint Intelligence Committee (including Central Intelligence Review)

29. The Joint Intelligence Committee (JIC)[6] is responsible for providing Ministers and senior officials with co-ordinated inter-departmental intelligence assessments on a range of issues of immediate and long-term importance to the UK's national interest. It is also responsible for producing the Strategic Priorities for Secret Intelligence Coverage (formerly known as the Requirements and Priorities for Secret Intelligence Collection). These are endorsed by the NSC, and set out in detail where GCHQ and SIS in particular (given their global remit) should allocate their effort, in terms of both geographic and organisational targets. These strategic themes and threats are revised on an annual basis and cover a three-year period.

30. In its Annual Report last year, the Committee said that it was important for there to be one clear tasking process, and recommended that the work of the JIC, and the Requirements and Priorities (R&Ps) process in particular, should be aligned with the strategic direction being set by the NSC. We therefore welcomed the Cabinet Office review, announced in January 2011, of the intelligence and security structures at the centre of government, including the role of the JIC.

31. In evidence to the Committee, the then National Security Adviser told the Committee that:

> *The creation of the NSC did make it necessary to review the function of the JIC. My own view is that it was necessary to review the function of the JIC anyway, because over the years it has become, I think, rather too stately and formal. I think the whole operational assessment has to be much fleeter.*[7]

---

[6] *The JIC draws its membership from senior officials in the Foreign and Commonwealth Office, Home Office, Department for Business, Innovation and Skills, Treasury, Ministry of Defence, Department for International Development and Cabinet Office. The Heads of the Security Service, SIS and GCHQ are members of the JIC. Representatives of other departments attend when necessary.*

[7] *Oral Evidence – National Security Adviser, 20 October 2011.*

The Cabinet Office review of the central intelligence machinery

The review recommended that:

- the NSC's priorities should be the lead driver of the JIC's agenda;
- the NSC (Officials) meeting is best placed to oversee the tasking of the JIC;
- the JIC should retain the scope to provide early warnings on issues outside of the immediate cycle of the NSC agenda;
- JIC 'Principals' (i.e. the Heads of Agencies) should meet once a month focusing on key NSC issues, judgements and papers;
- JIC 'Sub-Principals' would meet more frequently to consider issues of less immediate importance to the NSC or of importance to particular departments, or more short-term assessments;
- the JIC should produce a wider range of tailored intelligence products more focused and accessible to Ministerial readership;
- the wider intelligence assessment capability should be put more directly at the disposal of the NSC where appropriate;
- in supporting the NSC, the policy implications of analytical judgements should be identified in significant assessments given to Ministers through closer working between assessment and policy expertise in the Cabinet Office while respecting the independence of intelligence assessment from policy; and
- open source capabilities should be enhanced through the recruitment of a dedicated information specialist to improve the exploitation of open source material.

The impact

32. The review clearly positioned the JIC as sitting underneath the NSC and responding to the NSC's requirements in terms of producing assessments. This is sensible and in accordance with the NSC's role at the head of the intelligence machinery.

33. This relationship extends to the NSS and JIC R&Ps. Whilst the NSS sets a broad strategic direction, the JIC R&Ps provide the more detailed prioritisation. This is then overlaid by the weekly NSC, which dictates the more immediate repositioning of resources in response to particular events. The Director of GCHQ gave a useful description of how this works in practice:

> *… the Joint Intelligence Committee has continued to provide us, through its Requirements and Priorities process, with our annual priorities and focus. That tends to be quite a stable, quite a static, process. Then the National Security Council, with its weekly rhythm gives an opportunity for a more dynamic flexing of the system and of the information required from the agencies.*[8]

[8] *Oral Evidence – GCHQ, 1 December 2011.*

34. One of the more contentious recommendations of the review, however, concerned the inclusion of policy implications in intelligence assessments. It is essential that assessments are arrived at independent of policy considerations and the Committee was concerned that including any policy material may lead to boundaries being blurred and the objectivity of the JIC being undermined. We spoke to the Foreign Secretary about these concerns. He said:

> *… the JIC papers don't say, 'Well then, these are the policies that follow from that'. Of course within each department, we are looking at policies that are informed by intelligence. But I don't think we are getting a blurring of the lines, certainly not in the way that ministers make decisions.* [9]

A. It is imperative that policy implications and analytical judgements remain separate in any intelligence assessment provided to Ministers. We are reassured that Ministers recognise the importance of this distinction and that it will be maintained.

The 'Arab Spring'

35. The combination of the broad strategic direction set out in the National Security Strategy, the detailed longer-term consideration of priorities laid down in the JIC R&Ps and the more dynamic tasking by the National Security Council should provide an effective mechanism for directing the Agencies' efforts. The question is whether the system can cope with the unexpected, and indeed whether it should have been unexpected in the first place.

36. The rapid spread of the 'Arab Spring', from its start in Tunisia in December 2010, took many by surprise and presented a significant challenge to the UK intelligence community in terms of reprioritising its resources to respond to a rapidly escalating crisis.

Horizon scanning

37. In addition to the tasking mechanisms mentioned above, the National Security Strategy also lays emphasis, through the Strategic Defence and Security Review, on "*identifying threats and opportunities early, shaping developments and preventing new threats from emerging*".[10]

38. Whilst the R&Ps set in 2010 listed "*tackling global instability and conflict*"[11] as a strategic theme, ***, the low level requirement for production of intelligence across the Arab nations had resulted in a decrease in the resources committed to the area. SIS told us this year that their coverage of individual Arab countries had been falling for some time: their primary focus in the Middle East was Counter-Terrorism and Iran.[12] GCHQ told us that "*the Arab nations were one of the few areas where we were planning to draw down our effort pretty well comprehensively*".[13]

---

[9] *Oral Evidence – Foreign Secretary, 26 January 2012.*
[10] *Strategic Defence and Security Review, October 2010.*
[11] *Joint Intelligence Committee, Requirements and Priorities, 2010–13.*
[12] *Oral Evidence – SIS, 15 December 2011.*
[13] *Oral Evidence – GCHQ, 1 December 2011.*

39. We questioned SIS and GCHQ about whether the lack of coverage meant that they were taken by surprise. The Chief of SIS defended their performance, saying that no one had predicted what might happen:

> *They were inherently, I would argue, unpredictable that they would have happened in the way that they did and in the timing that they did, and there were no sort of secrets there which could have told us they were going to happen, because all the organisations that hold the secrets had no clue it was going to happen, and they were as caught by surprise as much as anyone.*[14]

Defence Intelligence said that whilst they had assessed regimes such as that in Egypt as "*unsustainable*", as a result of the "*demographics, the economic situation and a whole range of other factors*" they were unable "*to predict the spark which would cause it all*".[15]

B. The Committee recognises that it is often impossible to predict how and when events such as the 'Arab Spring' will begin, and it is understandable that the intelligence community was taken by surprise, as indeed were the governments in the countries affected. There is a question, however, as to whether the Agencies should have been able to anticipate how events might subsequently unfold, and whether the fact that they did not realise that the unrest would spread so rapidly across the Arab world demonstrates a lack of understanding about the region. Events over the past 18 months have shown the need for the intelligence and security Agencies to maintain a global coverage, in addition to the strategic priorities set by the National Security Council and the Joint Intelligence Committee.

[14] *Oral Evidence – SIS, 15 December 2011.*
[15] *Oral Evidence – Defence Intelligence, 8 March 2012.*

The 'Arab Spring'

- In December 2010, a young vegetable seller, Mohammed Bouazizzi, set himself on fire in Tunisia after his cart was confiscated and he was abused by the police. Unrest and anti-government violence quickly spread.
- The Tunisian President fled to Saudi Arabia in January 2011, ushering in the country's first democratic election.
- On 28 January, anti-government protests erupted in Egypt and a day later in Yemen.
- In February, Egyptian President Mubarak stepped down after the army refused to fire on protesters.
- The Gulf state of Bahrain saw a 'day of rage' protest in February, inspired by events in Tunisia and Egypt.
- On 15 February, the arrest of human rights activist Fethi Tarbel started a riot in the Libyan city of Benghazi, which later spread throughout the country.
- In March, Bahrain declared a state of martial law, and anti-government protests began in Syria's capital, Damascus. The Bahrain protests were quelled with the help of troops from Saudi Arabia and the Gulf states.
- The UN Security Council responded to events in Libya by authorising a no-fly zone over the country and military action to protect civilians from the army. The first NATO air strikes took place in March.
- In June, Yemen declared a state of emergency. The President later agreed to step down and transfer power to his successor, the former Vice President, Hadi.
- On 20 October, Colonel Gaddafi was captured and killed after the National Transitional Council forces took his home town of Sirte, ending a two-month siege.
- In November, the Arab League took the unprecedented step of suspending Syria from its membership.
- Egyptian parliamentary elections began in November, and took place over a six-week period. Presidential elections took place in May 2012.
- In March 2012, the UN and Arab League Peace Envoy Kofi Annan proposed a plan to end violence in Syria.
- In May 2012, the alleged massacre by forces loyal to the President of over 100 civilians, including 49 children and 34 women, in the town of Houla prompted the UK and other states to expel Syrian diplomats in protest.

The response

40. Events in January 2011 resulted in a rapid reversal in SIS's and GCHQ's plans to reduce their focus on the region and their allocation of resources. In evidence to us last year, the then National Security Adviser said:

Given the level of collection of intelligence material, the Agencies would not have been able to predict in January this year [2011] that in March, they would suddenly be asked to turn on a very high level of collection. I pay tribute to the agility that they showed in being able to do that.[16]

41. GCHQ had allocated ***% of its resources to the Middle East and North Africa targets during 2010/11 and expected to increase its allocation of effort to ***% in 2011/12.[17] Whilst this does not represent a significant increase, the primary shift has been within the Middle East and North Africa category towards those countries affected by the 'Arab Spring'.

42. GCHQ responded rapidly to events in Libya:

I think we were faster in responding to this than [some of our] counterparts were and… [they have] acknowledged that. I think we moved fast in terms of building up the team… within the space of a few weeks…[18]

The Foreign Secretary praised GCHQ's response, saying:

… their ability to turn the antennae in the right direction was quite remarkable and the volume of material produced by GCHQ on Libya was colossal: up to the point of an entire full red box every day for me to read of GCHQ reports on Libya.[19]

The quality of the analysis that GCHQ was able to produce so rapidly was a considerable strength.

43. SIS, similarly, had to respond from a near-standing start. They had allocated ***% of their resources to the Arab Nations target in 2010/11 and acknowledged that "*when the upheavals took place around the Arab world... our coverage of individual Arab countries had been falling for some time*." However, as the Chief explained: *"We were able, because of our global network, because of our partnerships in the region and because of a… stable of agents, we were able to turn that around quite quickly.*"[20] The Foreign Secretary acknowledged that "*it's harder from the point of view of human intelligence sources. Those don't appear overnight*" but said that he nevertheless considered that "*SIS did a good job after an initial difficulty, of getting people into places where they could give us information*".[21]

44. In addition to the work of SIS and GCHQ, Defence Intelligence (DI) was also heavily involved. DI told us:

Defence Intelligence played a key, nearly central, role in the Libyan campaign, primarily, to be fair, because we can direct a lot of the capabilities… very rapidly… There were two elements really to our involvement in the Libya operation. There was the initial evacuation of British citizens and then the longer military campaign that lasted many months and ultimately concluded successfully.[22]

---

16 *Oral Evidence – National Security Adviser, 20 October 2011.*
17 *Written Evidence – GCHQ, 30 September 2011.*
18 *Oral Evidence – GCHQ, 1 December 2011.*
19 *Oral Evidence – Foreign Secretary, 26 January 2012.*
20 *Oral Evidence – SIS, 15 December 2011.*
21 *Oral Evidence – Foreign Secretary, 26 January 2012.*
22 *Oral Evidence – Defence Intelligence, 8 March 2012.*

This contribution was particularly valued by Ministers, and the Foreign Secretary commented:

> *We really saw as ministers through the last year, through the Libya conflict, the value of Defence Intelligence. We started each day listening to the Chief of Defence Intelligence and then the JIC staff and we couldn't make our political decisions about Libya without really understanding the defence picture. So I think perhaps we have had direct experience, more than would be the case of ministers in recent years, of the value of Defence Intelligence.*[23]

Defence Intelligence is often on the sidelines in terms of the wider intelligence community, and the Committee is concerned that its work is often undervalued as a result. We were therefore pleased that the Libya campaign brought them to the forefront and that their contribution was recognised. We discuss the role of DI further on page 52.

45. Having had to respond so quickly, inevitably the Agencies' coverage has not been as full as they would have wished, and both GCHQ and SIS said that they were continuing to work hard to build this up. GCHQ said: "*We are working very hard, including with foreign partners, to improve our coverage in *** and I think that's looking promising. I think we are looking closely at the CT [Counter-Terrorism] dimensions of *** – the movements of weapons and that kind of thing – so that's an area of extra focus for us*."[24] SIS similarly acknowledged that they had been "*unable to provide detailed reporting on [the] Tunisia and Egypt crises*".[25]

An uncertain future

46. At the time of writing, the 'Arab Spring' has continued for well over a year. The situation in Syria remains uncertain with violent protests continuing and an unrelenting government response.[26] There is concern that Al-Qaeda in Iraq may gain a lasting foothold in Syria if there is a prolonged power vacuum, and also at the prospect of Syrian conventional and chemical weapons stockpiles falling into the hands of terrorist groups. This would pose a considerable threat both in the Middle East and more widely.

47. Elections have now taken place in Tunisia and Egypt, with Islamist parties performing strongly. In January 2012, the Foreign Secretary publicly welcomed the early signs of progress towards stable and open societies in the region:

> *We have… seen a groundbreaking shift in the willingness of members of the Arab League to show leadership in confronting crises in their midst. These are trends that must be supported. It is in our national interest to see stable and open societies emerge across the Middle East over time. It is true that parties drawing their inspiration from Islam have done better at the polls than secular parties and there are legitimate concerns about what this will mean… We must respect these choices while upholding our own principles of human rights and freedom and urging the highest standards… In standing up for the right of peoples to choose their own*

---

[23] *Oral Evidence – Defence Intelligence, 8 March 2012.*

[24] *Oral Evidence – GCHQ, 1 December 2011.*

[25] *Written Evidence – SIS, 3 October 2011.*

[26] *In December 2011 the UN High Commissioner for Human Rights reported that the death toll in Syria was over 5,000. More recent estimates put the death toll between 10,000 and 15,000 although, because the press and human rights organisations have little freedom of movement, the verification of any figures is difficult.*

representatives at the ballot box, we have to accept their choices and work with the governments they elect.[27]

48. We questioned the intelligence community about the impact of the outcomes of the 'Arab Spring' on the UK's national security. The Director of Central Intelligence Assessment in the Cabinet Office made the point that:

I think AQ has remarkably notably failed to take advantage of the Arab Spring. And in some way the positive sign that I would take out of it is that there is an alternative narrative available: that you can get rid of despotic regimes in ways that are not the same as the way that Al-Qaeda has been trying to persuade people to do. So actually the plus side is that you have got the makings of an alternative story, which could be very, very positive.[28]

49. The Director General of the Security Service noted that there were concerns as well as potential benefits:

Al-Qaeda did not create – and has not been able really to manage – any of the uprising, and it has been irrelevant to it, very largely. On the other hand, there are Islamist elements who are obviously in a much stronger position now than they were when they had Governments who repressed them, and there is a longer term question there… There is the question of security capacity and capability in the region; and whilst [some] organisations [in certain countries were]… in human rights terms, very bad, nevertheless they had a very significant impact on repressing Al-Qaeda activity. So there are risks from that, but there are also opportunities and you know, long term, if you have got a democratic pluralist Middle East, that would be a huge plus in national security terms."[29]

C. We commend the Agencies for their rapid reaction to the 'Arab Spring' once events became clear, and their very significant contribution to the UK's response. They demonstrated agility and flexibility in reprioritising their resources and providing the National Security Council with the intelligence it needed to form the UK response.

50. The nature of intelligence work is such that operational successes usually remain secret. Failures have the greater potential to become public. Whilst it is essential that the Agencies maintain flexibility and agility in fast-moving situations, they need to ensure that they still plan thoroughly and according to proper procedure. In one notable case this year, SIS failed to do so – with serious practical and diplomatic consequences. The failure of this operation prompted a 'lessons learned' exercise, the results of which indicated serious problems around lack of operational planning and leadership, delegation of responsibility to too junior a level and poor decision-making. SIS reported the detailed findings of the review to the Committee.[30]

---

[27] *Foreign Secretary, 'Freedom is still flowering in the Arab Spring', 13 January 2012.*
[28] *Oral Evidence – Director, Central Intelligence Assessment, 7 December 2011.*
[29] *Oral Evidence – Security Service, 8 December 2011.*
[30] *Written Evidence – SIS, 9 March 2011.*

***.[31,32]

51. The Foreign Secretary summed it up in the following terms:

> *One of the problems I think was that SIS felt they were under such pressure from ministers *** that they then didn't give what they would normally regard as all of the time and consideration to their plan and to the flexibility of their plan****.[33]

D. The Committee considers that the failure in one notable case this year demonstrates a lack of operational planning that we would not have expected from SIS and other participants. The imperative to take action quickly dominated at the expense of thorough and effective planning. It was an ill-considered approach that misjudged the nature and level of risk involved. We recognise, however, that SIS did implement a thorough review, following this failure, and appears to have taken the lessons seriously. We would have expected nothing less.

[31] *Ibid.*
[32] *Written Evidence – SIS, 28 November 2011.*
[33] *Oral Evidence – Foreign Secretary, 26 January 2012.*

COUNTER-TERRORISM

International Counter-Terrorism

52. Combating the threat from international terrorism remains the primary focus for the UK's intelligence and security Agencies. The pre-eminent threat remains that from Al-Qaeda and its affiliates; however, the nature of that threat has changed.[34] The death of Usama bin Laden, and the series of US drone attacks against senior leaders in the Federally Administered Tribal Areas of Pakistan (FATA), have weakened Al-Qaeda Core's capability.[35] According to the Centre for the Protection of National Infrastructure, "*AQ's senior leadership is crumbling*".[36] The Director General of the Security Service elaborated:

> *… there has been very considerable erosion of Al-Qaeda's senior leadership capability in Pakistan, and to some extent now in Yemen, as a result of drone strikes… the organisation has to spend a lot of its time trying to protect itself… it is much more difficult to take action if you are permanently in fear that you are going to be attacked. I think that has had a strategic impact on Al-Qaeda's senior leadership.*[37]

However, the Security Service assesses that the majority of the most dangerous UK-based extremist networks have had some form of contact with extremist groups in Pakistan. Some of these networks are capable of attack planning on the scale of 7/7. Pakistan-linked groups therefore continue to absorb considerable counter-terrorist resource, despite the shifts described above.

53. The growing threat from Al-Qaeda affiliates has led to an increased focus on countries such as Yemen and Somalia, and the activities of Al-Qaeda in the Arabian Peninsula (AQAP) and Al-Shabaab. As the Security Service told us: "*Somalia has become much more important as an issue than was the case five years ago. Pakistan [is] still a worry, but not quite as all-consuming as it has been.*"[38] ***.

54. In addition to this geographic change, the way in which terrorists are planning and commissioning attacks has diversified, with a greater number of so-called 'self-starters', i.e. groups or individuals who initiate attack planning and preparation without being directed to do so by Al-Qaeda leadership. ***.[39]

The policy response

55. The National Security Strategy[40] sets out the Government's approach to the broad range of security issues with further detail on its Counter-Terrorism Strategy set out in CONTEST. The stated aim of CONTEST is:

> *To reduce the risk to the United Kingdom and its interests overseas from terrorism, so that people can go about their lives freely and with confidence.*[41]

---

[34] *Al-Qaeda affiliates are: Al-Qaeda in the Arabian Peninsula (AQAP), Al-Qaeda in the Islamic Maghreb, Al-Qaeda in Iraq and Al-Shabaab.*

[35] *Al-Qaeda Core refers to the few hundred operatives in the FATA and, occasionally, in Afghanistan, including the group's senior leadership.*

[36] *CPNI Quarterly Threat Update 04/11, January 2012.*

[37] *Oral Evidence – Security Service, 24 November 2011.*

[38] *Ibid.*

[39] *Ibid. This redaction is made on sub judice rather than national security grounds.*

[40] *Cm 8123.*

[41] *Ibid.*

CONTEST covers four distinct areas:

i. Pursue: to stop terrorist attacks;

ii. Prevent: to stop people becoming terrorists or supporting terrorism;

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

iv. Prepare: to mitigate the impact of a terrorist attack.[42]

The work of the intelligence and security Agencies focuses on the Pursue and Protect strands of CONTEST.

The Agencies' response: in the UK

56. The Security Service allocated 72% of its overall resources to ICT during 2010/11. This was unchanged from the previous year, but the increase in the Security Service's budget meant that the actual spend on ICT increased slightly. The Service expected its relative allocation of effort on ICT to remain steady in 2011/12, but that spending would rise by a further 10%.[43]

57. This increase in funding has meant that, despite the diversification of the threat, the Security Service reports that its intelligence coverage in the UK remains steady. Overall, it "*is in a better position to identify and pre-empt hostile plots developing within the UK*"[44] and the total number of plots remains "*broadly stable*".[45] Nevertheless, that number remains high, and when a surge in effort is required on a particular plot, lower-priority investigations must be suspended.

58. This may seem surprising given the growth of the Agencies over the last few years (the Single Intelligence Account doubled in cash terms over the last decade). However, it reflects the intensive nature of intelligence investigations, and the amount of data generated by the various leads that have to be followed up. The Director General of the Security Service said:

> *But this is in the nature of the sort of work we are in and the critical thing is to have a rational and managed way of doing our priorities, which I am confident that we have…*[46]

59. It is clear that coverage of terrorist groups is by no means comprehensive. Resources need to be shifted to target the most pressing issues, ***.[47] Nevertheless, they have had notable successes: nine men were jailed in February 2012 for plotting to bomb the London Stock Exchange and establish a terrorist training camp.

60. As well as the pressures that the number of terrorist plots places on the Service's resources, a further issue is the reduction in the effectiveness of the disruptive tools that can be employed either by the Service or by the police, the UK Border Agency, the Serious

---

[42] *Cm 7547.*

[43] *Although the Service received a 'flat-cash' settlement in the 2010 Spending Review, it has been given additional funding for Counter-Terrorism work and Terrorism Prevention and Investigation Measures (TPIMs).*

[44] *Written Evidence – Security Service, 30 September 2011.*

[45] *Oral Evidence – Security Service, 24 November 2011.*

[46] *Ibid.*

[47] *Written Evidence – Security Service, 30 September 2011.*

Organised Crime Agency, the Crown Prosecution Service and others.[48] It is particularly concerning that the Service reports that:

> *Despite some notable successes, our disruptive impact on hostile individuals and networks has reduced over the period. Better upstream intelligence has helped us uncover some UK-based plots at a less advanced stage, but earlier action can mean less evidence on which to prosecute… A great deal of effort has gone into finding ways to maintain the value of the disruptive tools, with significant success. Nevertheless, the net effect of all these developments is that we now have to work harder, and invest more resource, to disrupt groups and all this absorbs investigative effort and sharpens prioritisation yet further.*[49]

The Agencies' response: overseas

61. In terms of overseas work, the Committee has been told that an increasing amount of the Security Service's casework has an 'upstream' element (i.e. aspects such as attack planning, preparation or direction occurring outside the UK, and terrorist groups with little or no presence in the UK). However, there are inherent difficulties in attempting to investigate terrorist groups based in countries such as Yemen and Somalia, as opposed to the UK.

62. This has necessitated greater collaboration between the three Agencies: whilst SIS and GCHQ have always supported the Security Service's investigations where they have 'upstream' elements, a new tri-Agency approach has now been adopted. This sees the Security Service taking the formal lead for overseas investigations, but with SIS and GCHQ retaining control of operational targeting. Although the logistical arrangements will vary, generally this sees Security Service officers embedded with their SIS and GCHQ counterparts.

63. SIS's effort on ICT continued at 35% in 2010/11, and was projected to remain broadly steady in 2011/12. The Chief explained how this effort was allocated:

> *… we have to balance the immediate short term priorities, which by and large tend to be, not surprising, the priority of the Security Service and the police in this country, with the need for longer term investment in these targets and that's an issue which we have to manage.*[50]

64. SIS also underlined that the breadth and range of its reporting was not where it would wish it to be. Although coverage has improved significantly over the last few years, SIS reported: "*We have not achieved the full range and assurance from 'tripwire' reporting HMG needs on the major sources of upstream AQ threat.*"[51] The need to support specific Security Service investigations means that resources are diverted away from building a more general picture of the threat and activities of terrorist groups. This should not, however, detract from the successes that have been seen over the past year, including

---

[48] *The Security Service seeks to disrupt terrorist subjects of interest/networks in order to mitigate (or manage) the risk they pose to national security. As far as possible, the Service always aims to effect a successful prosecution against terrorist subjects (working alongside the police and Crown Prosecution Service to achieve this). This cannot be realised in all cases. Where Service investigations reveal involvement in (non-terrorism related) crime this may present an opportunity for the police to achieve a disruption. Direct Security Service engagement with a subject of interest – either overt or covert – can also have a disruptive effect. Other non-prosecution options available to the police, UK Border Force and HM Treasury include TPIMs, exclusions, immigration actions (e.g. deportation, deprivation of nationality) and asset freezing. The Government's efforts to deport Abu Qatada, who is considered to pose a threat to the UK, is an example of an attempt to use such tools.*

[49] *Written Evidence – Security Service, 30 September 2011.*

[50] *Oral Evidence – SIS, 15 December 2011.*

[51] *Written Evidence – SIS, 3 October 2011. 'Tripwire' reporting refers to early warnings of attack planning or preparation.*

disrupting planned terrorist attacks in Asia, and contributing to the arrests of terrorist suspects involved in attacks in Africa.

65. ICT is also the highest priority for GCHQ and SIS, accounting for around a third of the effort of both. As with SIS, most of GCHQ's work in this area is in support of the Security Service. During 2010/11, it provided reporting on the activities of Al-Qaeda and its affiliates, and the activities of ***. In addition, GCHQ responded to tasking from policy departments for any indications of terrorist activity in ***, although it admitted that as it had been planning to reduce effort in this area of the world prior to the 'Arab Spring', this was "*an area of extra focus*" that would require sustained effort to improve coverage. However, GCHQ underlined that coverage and reporting was not solely dependent on staff numbers:

> *… the impact that we can make is only partially dependent on the number of analysts we have working on it. It's also about new accesses, new tradecraft, new techniques and new tools… the challenge is for us to make the most of that technology lead that we've got to compensate for some of these small reductions in effort*.[52]

E. The Agencies have continued to see notable successes in their Counter-Terrorism work. It is clear that this is becoming more challenging and, despite increases in resources, they still face difficult decisions when prioritising their efforts against the most pressing threats. Given that the Agencies' recent growth will not continue over the coming years, the challenge will be to get the most out of current resources through more innovative – and where appropriate collaborative – working. The Committee welcomes the progress the Agencies are making in this regard.

The Olympic and Paralympic Games

66. The Olympic and Paralympic Games represent a critical security challenge for the police and the Agencies during 2012. The Committee reported last year how the Security Service saw the Games as central to its planning for the early years of the current Spending Review period, and that these plans included recruiting additional intelligence officers and moving resources into countering the threat of a terrorist attack.[53] Earlier this year we asked the Director General for an update on these issues, and he explained that the Service had identified three potential sources of threat:

- Al-Qaeda and its affiliates planning an attack on the Games and/or participants, especially US or Israeli nationals;
- republican terrorist groups, either through an attack or a hoax to cause disruption rather than mass casualties; and
- clashes between rival groups or ethnicities that would be present in London during the Games but who ordinarily would not be considered a threat to the UK.

67. The Security Service has planned on the basis of an increased terrorist threat during the Games, resulting in greater volumes of intelligence to be analysed and responded to, coupled with a shorter turnaround time and a lower risk threshold than would normally be applied to such intelligence.[54] The Security Service told us it has planned on the basis

---

[52] *Oral Evidence – GCHQ, 1 December 2011.*

[53] *Cm 8114.*

[54] *Although at the time of writing the terrorist threat level to the UK from international terrorism is SUBSTANTIAL, the overall security arrangements for the Games have been based on the assumption of the threat level being SEVERE.*

of having to cope with double the normal volume of new intelligence leads, with peaks of possibly four times greater than usual.

68. In addition to this, there were two other aspects of the preparations that increased pressure on the Security Service considerably:

i. the burden of the accreditation process (which requires all 540,000 applications from those working at the venues, as well as officials, volunteers and team members, to be checked against relevant databases to identify anyone whose presence may be a threat to national security); and

ii. the need for extensive briefing of and liaison with foreign partners, as foreign intelligence services from the more than 200 nations represented at the Games are expected to send representatives with their delegations for co-ordination and security purposes.

The Agencies' response

69. In preparation for the Games, the Security Service reduced its effort on work of a lower priority so that effort could be redirected into countering the potential threats the Games will face. It also began a 'clearing the decks' exercise[55] which involves reviewing existing casework in order to minimise the overall risk before the Games. In some cases this may lead to temporary disruptions being taken against terrorist groups at an earlier stage than would normally be ideal. The Service also suspended some of the investment programmes that were under way in order to ensure that IT resilience could be guaranteed.

70. The Committee explained in its 2010–2011 Annual Report that the Security Service would have to move staff from other areas to undertake Counter-Terrorism work during the Games. We reported that the Service would have to reduce substantially its work on *** during the period of the Olympics.[56] We concluded that the diversion of resources to service the demands of the Olympics exposed the UK to greater risk, and that the National Security Council "*must take such steps as are necessary to minimise the risk to the UK*".[57] However, we were told in October 2011 that ***.[58]

71. We questioned the Home Secretary and the National Security Adviser about the situation. The Home Secretary confirmed that she had discussed the issue with the Director General of the Security Service, but said:

> *Well you have to prioritise the threats that you are dealing with, and in relation to the safety and security of the Olympics obviously that means that we look specifically at the international counter-terrorist threat… It is not the case that we are talking about not having individuals doing that [other] work.*[59]

The Director General provided further details on staffing arrangements that were being put in place prior to the Olympics:

---

[55] *This exercise is still under way and will continue throughout the Games.*
[56] *Cm 8114.*
[57] *Ibid.*
[58] *Written Evidence – Security Service, 3 October 2011.*
[59] *Oral Evidence – Home Secretary, 19 January 2012.*

*… we are taking people off issues and areas of work which are important, but not urgent, and moving them into operational response; those who have got the right skills. And then to some extent, back filling where we can. So stopping doing lots of other things and concentrating on this. We are going to take people out of ***, we are going to take people out of personnel, we are going to take people out of IT…*[60]

72. The National Security Adviser confirmed that this issue had not been raised at the National Security Council, and added:

Of course there will be greater risk. But with finite resources and a major national priority requiring greater effort over a defined period of time, it is inevitable that there will have to be a greater risk-taking in some parts of the Security Service business, and I think we have to depend on the professionalism of the Director General to decide where that risk can most safely be taken…[61]

F. We recognise that the Security Service has taken all possible measures to make available the necessary resources during the period of the Olympic and Paralympic Games, but remain concerned at the risk that is being taken in some areas and the vulnerability of the UK at this critical period.

73. In support of the Security Service and the police, SIS has increased the resources and GCHQ has plans to "*surge*" the resources they put into Counter-Terrorism, to try to give warning of any plots and also to react to any attack as necessary. SIS told us that the prioritisation of the Olympics would affect other counter-terrorist work, and GCHQ told us it has plans to create a pool of 20% of its non-Counter-Terrorism and non-serious crime analysts "*who can be dynamically deployable between the normal mission and the Olympic response as necessary*".[62]

74. In addition to the diversion of resources and deferral of investment, the Agencies have taken additional measures to increase capacity. All three Agencies have had to change working patterns in order to accommodate the additional pressures, including imposing leave restrictions, freezing non-essential staff-moves, and increasing the scale of 24/7 and extended-hours operating before and during the Games. All these increase capacity to deal with the greater flows of intelligence, but they have been described to us as "*having quite a significant impact*" and being "*very difficult for some people*",[63] particularly in terms of arranging childcare over the summer period. It is clear that the greatest burden will fall on the Security Service.

G. The Olympic and Paralympic Games have placed all three Agencies (particularly the Security Service) under unprecedented pressure this year. The Committee recognises the exceptional effort that has been required from the staff of all three during this time.

Review of Counter-Terrorism powers

75. The Committee reported last year on the new regime of Terrorism Prevention and Investigation Measures (TPIMs) that would replace Control Orders. We noted that the

---

[60] *Oral Evidence – Security Service, 24 November 2011.*
[61] *Oral Evidence – National Security Adviser, 20 October 2011.*
[62] *Oral Evidence – GCHQ, 1 December 2011.*
[63] *Oral Evidence – Security Service, 24 November 2011.*

powers available to the Government under TPIMs were less restrictive than those under Control Orders, and the Security Service would receive additional funding to offset the increased burden that would be placed on it.

76. This transition took place in January 2012, following the passage of the relevant legislation. The delay between the announcement that Control Orders would be abolished (which was made in January 2011) and implementing the new powers was due to the need to increase resources available to the police and Security Service to compensate for the additional investigative work they would be require to undertake.

77. This year the Committee has reviewed the TPIMs proposals in more detail, including how decisions were made regarding the level of additional funding to be made available to the Security Service, and also the preparations for the transition. We asked the Home Secretary whether she was satisfied that the new powers meant there would be no increase in risk. We were told:

> *… when you ask Home Secretaries to make guarantees about risk, that's something that I have to say that I don't do in most circumstances and therefore would be reluctant to do in these as well.*[64]

The Director General of the Security Service echoed this point:

> *I would not be able, hand on heart, to say there will be no increase in the risk; but I don't think there will be, overall, a substantial increase in risk. And given the total risk in the system which is still considerable, I do not think this is a really major step change.*[65]

78. However, the Home Secretary considered that the extra money that was being provided would contain the risk:

> *But I'm confident that… we have, with the extra resources that [the police and Security Service] have available, the ability for them to [manage the risk] in a way that is what I believe is right for public safety.*[66]

The Independent Reviewer of Terrorism Legislation, David Anderson QC, broadly supported this position, noting that whilst TPIMs "*are unlikely to further the requirements of national security – rather the reverse… by making significant extra resources available for covert investigative techniques, the Government has sought to ensure… that there should be no substantial increase in overall risk.*"[67]

79. In the case of the Security Service, the extra resources amounted to £***m over four years. The Committee had assumed that this money would be allocated to monitor those individuals who would move across from Control Orders to TPIMs, and thus was based on a calculation of net additional cost per individual. Instead, we were told that the Service "*judged that… we required a significant increase in <u>overall</u> intelligence collection and*

---

[64] *Oral Evidence – Home Secretary, 19 January 2012.*
[65] *Oral Evidence – Security Service, 24 November 2011.*
[66] *Oral Evidence – Home Secretary, 19 January 2012.*
[67] *David Anderson QC, 'Report on Control Orders 2011', 26 March 2012.*

investigative capacity, not just to cover individuals subject to TPIMs".[68] The extra money was not, therefore, in any way ring-fenced for particular individuals or investigations.

80. Given that this means that the figure of £***m was, therefore, a general estimate, the Committee is concerned that it is difficult to assess whether it is appropriate. The Security Service has itself acknowledged that "*this is not an area that lends itself to precision*".[69] The level of funding may need to be reviewed to ensure that the increase in Security Service capability is sufficient to minimise the increased risk the TPIMs regime brings.

81. Regardless of how this level of funding was arrived at, it was essential that it was in place in sufficient time to allow the Security Service and police time to prepare. However, there have been numerous media reports suggesting that there were delays in recruiting and training additional specialist staff (such as surveillance officers), and that the police had consequently requested a delay in introducing TPIMs.[70] We asked the Home Secretary what the current position was. She confirmed that the police had not spent all the money made available to them in anticipation of the introduction to TPIMs. The Security Service gave more detail, saying:

> *I think for various reasons, the police had slightly more hoops to jump through, in order to get the funding in place; as a result of which, it has been slightly harder for them than it perhaps has been for us to get advanced on that increase in resources. We are not going to be 100 per cent there within the timeframe, but I think we are in a better position than the police… clearly we would rather be in a situation where the police resources were fully in place, or otherwise were in place, as far as ours are. But they are slightly behind us; and that increases the risk element.*[71]

H. The Committee is concerned about the potential increase in overall risk as a result of the introduction of the Terrorism Prevention and Investigation Measures (TPIMs) regime. The lack of any direct correlation between risk levels and the additional funding made available to the Security Service and police to prepare for this only adds to our unease, as do the delays in putting the funding in place prior to the transition from Control Orders.

'Enhanced' TPIMs

82. On 1 September 2011, the Government published a draft 'Enhanced' TPIMs Bill that would allow the Home Secretary to impose, in exceptional circumstances, more wide-reaching restrictions than those available under the TPIMs regime. These would include residence measures, movement restrictions, imposition of a curfew and restrictions on the use of communications or associations by terrorist suspects. These proposals have not yet been subject to pre-legislative scrutiny and will not proceed through the full legislative process until exceptional circumstances arise that might trigger the need to apply for such powers.

83. We asked for more detail on the Home Secretary's thinking behind what might constitute the circumstances in which 'Enhanced' TPIMs were considered necessary. The Home Secretary told us:

---

[68] *Written Evidence – Security Service, 8 December 2011 (emphasis in original).*
[69] *Written Evidence – Security Service, 31 January 2012.*
[70] *See for instance 'Met reveals its fears over keeping track of terror suspects', Evening Standard, 5 December 2011.*
[71] *Oral Evidence – Security Service, 24 November 2011.*

I don't think it's right to set out a sort of, 'Here are the circumstances in which it would definitely be right to come to Parliament with', or, 'If this happens we will come to Parliament with an Enhanced TPIM.' I think we have to have that flexibility. I mean, one might imagine a circumstance where if a number of attacks had taken place and there was some evidence that further attacks might be down the line, that in those circumstances, for example, that might be one set of circumstances where one might come to Parliament.[72]

84. The Director General of the Security Service appeared sceptical about the likelihood of 'Enhanced' TPIMs being invoked, even if the national threat level were to rise, telling the Committee:

I can't really envisage these things being used, to be perfectly frank… If the situation had deteriorated very severely, very badly, then we would need to consider whether that was the case. Merely a return to a SEVERE threat, I do not think would constitute the sort of exceptional circumstances where we would need to try and operationalise this power… I do not think [the trigger point for invoking 'Enhanced' TPIMs] has been worked through in any detail.[73]

I. Given the increased risk associated with the TPIMs regime, we welcome the Government's move to make additional powers available should the circumstances demand. However, the 'Enhanced' TPIMs proposals do not appear to be practical or workable, and it seems unlikely that they would ever be implemented.

Northern Ireland-related terrorism

85. In our last Annual Report, we noted the increasing threat from Northern Ireland-related terrorism, which had resulted in a greater number of attacks in 2009 and 2010 than in previous years. We asked the Director General for an update on the current position. He told us that he was "*very cautiously optimistic about the trajectory of the threat over the last 12 months*",[74] noting that there had been a reduction in both the number and scale of the attacks in 2011 (26 against national security targets in 2011, compared with 40 in 2010).

86. The Committee was told that the reduction was the result of intense activity by the police in Northern Ireland, who had made over 200 arrests for terrorism-related offences. This had had a cumulative impact on the dissident groups. Nevertheless, the Service has underlined that it continues "*to carry a high level of risk from the Dissident Republican threat in 2011/12*":[75] the killing of a Police Service of Northern Ireland officer in April 2011 demonstrated that a high level of intent and capability remains.

87. We reported last year that the Security Service had been increasing the amount of resource devoted to Northern Ireland-related terrorism. In 2010/11, this accounted for 17% of the Service's overall effort, an increase from 15% the previous year and 13% the year before. The Director General told us that "*the overall effect of this is, I think, that we have a better coverage than we had 12 months ago*".[76] However, we were also told that resources are unlikely to increase further in the future:

---

[72] *Oral Evidence – Home Secretary, 19 January 2012.*
[73] *Oral Evidence – Security Service, 23 November 2011.*
[74] *Oral Evidence – Security Service, 24 November 2011.*
[75] *Written Evidence – Security Service, 30 September 2011.*
[76] *Oral Evidence – Security Service, 24 November 2011.*

Our working assumption is that we will maintain our resources at the level they are at, but we are not intending significantly to increase in Northern Ireland, maybe not to increase at all… Our aim is to maintain and continually, if possible, increase this pressure and try and squeeze the energy out of the threat over the coming three years, with the aim of having a significantly improved position by 2015.[77]

88. In 2010/11, the Service saw a mixture of both successes and setbacks. One key operation resulted in the conviction in Lithuania of Michael Campbell – a senior Real IRA (RIRA) figure – on charges of attempting to procure military grade weapons and explosives. The Service called this "*a significant success… [which] has had an adverse impact on [RIRA's] ability to procure weaponry overseas*".[78] In addition, the Service supported the Police Service of Northern Ireland investigations that led to the conviction of the murderers of Constable Steven Carroll, who was killed by the Continuity IRA in 2009, and which secured the conviction of Brian Shivers for the Massareene Barracks murders of 2009. By contrast, prominent republican Colin Duffy was acquitted of involvement in the latter attack and Desmond Kearns was acquitted – on grounds of entrapment by the Service – of smuggling weapons for RIRA (although two other men were convicted of the charges brought against them). The Director General predicted that a Duffy acquittal would be "*good for [dissident republican] morale, and that is significant in this sort of thing*".[79]

89. Whilst the threat of attacks in Northern Ireland remains high, we also discussed with the Director General whether he had seen any change in the intent of the terrorists to mount attacks in Great Britain. He told us:

***.[80]

Dissident groups pose a threat, including potentially over the period of the Olympics.

90. ***.[81] ***.[82]

91. One of the issues that we discussed with the Director General this year was the security of officers in Northern Ireland. Although all members of staff are potential targets for terrorists, this risk is seen as greater in Northern Ireland owing to the high level of dissident republican activity. The Service reported that it has carried out work to "*increase the effectiveness of personal security in Northern Ireland*".[83]

***.[84]

Counter-radicalisation

92. The previous parts of this section relate to the Agencies' work on the Pursue and Protect strands of CONTEST. Responsibility for the Prevent strand lies with the Office for Security and Counter Terrorism (OSCT) in the Home Office. In 2011, the Government described the Prevent strategy as "*flawed… [confusing] the delivery of Government*

---

77 *Oral Evidence – Security Service, 24 November 2011.*
78 *Written Evidence – Cabinet Office, 4 November 2011.*
79 *Oral Evidence – Security Service, 24 November 2011.*
80 *Ibid.*
81 ***.
82 ***.
83 *Security Service Annual Report and Accounts 2010–11.*
84 *Oral Evidence – Security Service, 23 February 2012.*

policy to promote integration with Government policy to prevent terrorism".[85] It reviewed Prevent, publishing a revised strategy in June 2011.[86]

93. The strategy is guided by the need to separate Counter-Terrorism (to be co-ordinated by the Home Office) from the wider integration policy (to be co-ordinated by the Department for Communities and Local Government); and to increase monitoring and evaluation of projects and institutions funded by Prevent to address the risks of radicalisation.

The aims of the revised Prevent strategy

First, we will respond to the ideological challenge of terrorism and the threat from those who promote it. In doing so, we must be clear: the ideology of extremism and terrorism is the problem; legitimate religious belief emphatically is not. But we will not work with extremist organisations that oppose our values of universal human rights, equality before the law, democracy and full participation in our society. If organisations do not accept these fundamental values, we will not work with them and we will not fund them.

Second, we will prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support. We will build on the successful multi-agency 'Channel' programme, which identifies and provides support for people at risk of radicalisation.

Third, we will work with sectors and institutions where there are risks of radicalisation. Here, progress has been made in recent years, but it is patchy and must be better. So we will work with education and healthcare providers, faith groups, charities and the wider criminal justice system. We will also work to tackle the challenge of radicalisation on the internet.[87]

94. Within OSCT, the Research, Information and Communications Unit's (RICU's) role is to challenge terrorist and extremist activities and communications at the local level through counter-ideological projects. RICU operates both in the UK and in priority countries abroad, and reports to both the Home Office and the Foreign and Commonwealth Office.

95. This Committee has expressed concerns in the past regarding work on Prevent and the role of RICU, and, in particular, the lack of clear measures against which to assess the success of Prevent. In its 2010–2011 Annual Report the Committee concluded that "*It is… essential that there is some mechanism by which the success of work on the Prevent strand of CONTEST – and the benefits of RICU in particular – can be evaluated*".[88]

96. The Home Secretary told us that, as a result of the review of Prevent, RICU has a new focus:

---

[85] *Cm 8092.*
[86] *Ibid.*
[87] *Ibid.*
[88] *Cm 8114.*

- Clearer definitions and approaches to measuring impact (as opposed to volume) were being considered. This included "*measurements of the impact that the interaction has had on the individuals concerned to get a much better measure of the outcome of intervention*". However, she acknowledged that "*if you are going out with a message to a wider group it's harder to find the way to evaluate the impact of that message*". One option which was being considered was the use of focus groups "*to try and get a measure of the actual impact that the message that is given has on the recipients as opposed to simply how many outlets it has*".[89]

- In terms of communication strategies to respond to, and challenge, extremist and radical views, RICU would now be expected to "*deliver sharper and more professional counter-narrative products*".[90] Since June 2011, RICU has focused on engaging credible civil society organisations in order to encourage these organisations to challenge radical and extreme views in their local communities. The Home Secretary assured us that – particularly given previous concerns about the groups that were receiving funding – RICU had now recognised the importance of choosing credible groups with good leadership:

  > *Often it is more effective to be working through groups that are recognised as having a voice and having an impact with that voice, rather than it being seen to be government trying to give a message. Indeed, it's always better to be using those people to whom people look naturally to hear the message, rather than simply doing it as RICU itself.*[91]

- Work was also being developed to challenge extremism online. The Home Secretary said RICU was "*currently road-testing some quite innovative approaches to counter-ideological messages*".[92]

- RICU was also working with organisations overseas: this work is co-ordinated by the Foreign and Commonwealth Office. The Home Secretary explained that it was focused on specific countries where the UK judged the threat of terrorism and radicalisation to be strongest: "*it has more been a question of identifying those countries which are particular sources of potential threats into the UK and working in those countries. Obviously Pakistan is a country where RICU particularly works*."[93]

J. Prevent is a key strand of the Government's Counter-Terrorism Strategy and the Committee will continue to monitor this important work. The Research, Information and Communications Unit's counter-radicalisation work is progressing, albeit slowly. We understand that counter-ideological work may take some time. However, the Committee continues to be concerned about the lack of measures to assess the effectiveness of the strategy. Whilst we recognise the difficulties involved, it is nevertheless important that ways are found to identify and assess the results of this work and the resources being used.

---

89 *Oral Evidence – Home Secretary, 19 January 2012.*
90 *Cm 8092.*
91 *Oral Evidence – Home Secretary, 19 January 2012.*
92 *Ibid.*
93 *Ibid.*

CYBER SECURITY

97. In our 2010–2011 Annual Report, we welcomed the fact that the Government had listed cyber security as a Tier One risk in the National Security Strategy.[94] The increased profile was accompanied by funding of £650m over four years – primarily to fund projects under the National Cyber Security Programme (NCSP). This aims to transform the UK's cyber security skills and capabilities by 2015. Over half of this money has been allocated to the intelligence and security Agencies (with the bulk of it allocated to GCHQ).

In November 2011, the Government launched its Cyber Security Strategy which described how a transformation in the UK's cyber security capabilities is to be achieved. The strategy states:

> *Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.*[95]

This 'vision' is to be delivered by focusing on four overarching objectives:

- ***Objective 1:*** *The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace.*
- ***Objective 2:*** *The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace.*
- ***Objective 3:*** *The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies.*
- ***Objective 4:*** *The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.*[96]

Ministerial responsibility

98. Last year, we were concerned that there was insufficient clarity in terms of Ministerial responsibility and accountability for cyber security. We welcomed the transfer of responsibility from the Home Office to the Cabinet Office, which is better suited to overseeing cross-government initiatives and programmes. While the situation now is much clearer than it was previously, we remained concerned as to whether there was still potential for confusion, given the Foreign and Home Secretaries' overall responsibilities for the Agencies. This is particularly important for GCHQ, which is the lead Agency on cyber security. We asked the Foreign Secretary how well the new division of responsibilities was working. He said:

> *I don't think there is any confusion. There are a number of ministers with responsibilities in this area, but there needs to be because it does go across government to such an extent. I think the responsibility for cyber security has to be at a central point, so it is right that Francis Maude has the responsibilities that he has. That's not inconsistent with my oversight of GCHQ… it is me who signs*

[94] *Ibid.*
[95] *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, November 2011.*
[96] *Ibid.*

the authorities of GCHQ and I'm responsible within the government for GCHQ. But I think cyber security needs pulling together across all the departments. We have a very useful ministerial coordinating group on cyber security which I chair… including ministers from the Home Office, DCMS and so on.[97]

London Conference on Cyberspace

99. On 1–2 November 2011, the Foreign Secretary hosted the London Conference on Cyberspace. This was one of the first major attempts to establish international agreements covering the full range of opportunities and threats posed by the increasing use of cyberspace. The conference was attended by over 700 participants (and even more online) from 60 countries and covered a number of key themes in relation to the internet including:

- economic growth and development;
- social benefits;
- safe and reliable access to the internet;
- international security; and
- cyber crime (including the international Convention on Cybercrime).[98]

100. In his closing remarks to the conference, the Foreign Secretary summarised the conference's conclusions on international security including: the agreement that governments must act proportionately in cyberspace and in compliance with international law; that there should be stronger co-operation and collaboration between states; and, that there was no appetite for new international laws. The Foreign Secretary urged countries to join the Convention on Cybercrime – originally a Council of Europe agreement, but now with many non-European signatories – to govern freedoms and security in cyberspace. The Foreign Secretary told us:

I think we made a good start… I think we succeeded as the UK in setting the right tone and the right content of discussion and so on. We placed a great emphasis on freedom as well as security and it was not a paranoid, defensive discussion among governments about how to stop people finding out things. It was structured as almost a celebration of all the opportunities that cyberspace and the internet bring to the world, but recognising that that may also bring some challenges.[99]

The Agencies' work on cyber security

101. Over half of the £650m funding for the National Cyber Security Programme (NCSP) has been allocated to the intelligence community, with the majority allocated to GCHQ. This funding will be used for a number of projects, including:

- In GCHQ: to expand work on protective cyber security advice and information assurance; to improve the detection and analysis of cyber attacks including cyber crime; to consider intelligence operations in cyberspace; to improve co-operation with international allies and partners; and to work with the Ministry

[97] *Oral Evidence – Foreign Secretary, 26 January 2012.*
[98] *www.fco.gov.uk/en/global-issues/london-conference-cyberspace/cyber-conference-details/*
[99] *Oral Evidence – Foreign Secretary, 26 January 2012.*

of Defence to set up a Joint Cyber Unit hosted at GCHQ to develop new tactics, techniques and plans to deliver military effects, including enhanced security, through cyberspace.

- In SIS: to develop its role as an 'enabler' for GCHQ's cyber work ***.
- In the Security Service: to develop and enhance its cyber section, in particular bringing together its cyber investigations and protective security work into a single team. Its work focuses on investigating cyber threats from hostile foreign intelligence services and working with UK victims. In addition, its protective security work has been broadened beyond the Critical National Infrastructure to include other priority areas of the UK private sector.

102. Since cyber techniques are largely a tool for undertaking the Agencies' day-to-day work, and therefore cut across most areas of their business, there are no precise figures available for the Agencies' effort in this area. However, a very significant proportion of GCHQ's work has a cyber-related element and in the other Agencies it plays a growing part in their work against a range of targets.

103. The NCSP was established more than 20 months ago and the Committee has therefore been keen to ascertain what specific outcomes have been achieved thus far. While there are many ways to categorise the different aspects of cyber security, we have considered progress made against cyber security activities.

104. The Government's protective security work in this field is well established, primarily through the work of GCHQ's Communications-Electronics Security Group (CESG). The focus of this work is what could be described as the defence, or security, of computers and networks: ensuring that the barriers against cyber attacks are strong, that vulnerabilities are reduced and that networks are monitored so that attacks can be spotted.

105. GCHQ estimates that approximately 80% of successful cyber attacks could be thwarted by simple computer and network 'hygiene'.[100] This involves individuals, businesses and government taking steps such as using appropriate security software and ensuring operating systems are kept up to date. It also involves using 'strong' passwords and other authentication measures, using different passwords on different websites, installing only trusted software and being cautious in relation to unsolicited emails. These simple measures are applicable to government IT systems, in the commercial sector and for individuals at home. The key to countering these cyber attacks therefore lies in the availability and effectiveness of counter-measures (such as anti-virus and firewall software) and the education of computer users.

106. The work of CESG, and that of other bodies such as the Centre for the Protection of National Infrastructure (CPNI), on this aspect of cyber security continues to be highly valued by both the public and private sectors.

[100] *Oral Evidence – GCHQ, 1 December 2011.*

K. The provision of Information Assurance advice to government, businesses and the public has the potential to generate the greatest improvement in UK cyber security for the least cost. The Communications-Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI), among others, continue to provide an invaluable service to businesses and government departments in this regard. Nonetheless, educating users and individuals about basic information security has significant potential and should be a greater focus for the National Cyber Security Programme.

107. We reported last year that CESG continues to suffer a funding shortfall and that this has led to GCHQ having to provide subsidies of several million pounds a year. We understand that the shortfall has reduced significantly in both 2010/11 and 2011/12 due to short-term funding from the NCSP and one-off payments and we welcome this additional investment. However, the problem of a funding shortfall for CESG's work in support of cross-government ICT programmes remains.

L. We recommended last year that the Deputy National Security Adviser should prioritise the development of an effective funding model for the Communications-Electronics Security Group (CESG). To a certain extent the problem has been addressed through short-term funding arrangements. However, the importance of CESG's Information Assurance work requires that a long-term funding model must be established.

108. GCHQ, as the technical experts in this field, focuses on the 20% of cyber attacks that demonstrate greater levels of sophistication and which are more likely to be state-sponsored, or relating to serious crime. Its Cyber Defence Operations team – formerly the Network Defence Intelligence and Security Team (NDIST) – has significantly improved coverage of cyber attacks on UK interests worldwide. It detects and analyses cyber attacks in order to understand the vulnerabilities which are being exploited, seeks to attribute attacks to their source, to help develop counter-measures and, in turn, improve the protective security advice offered by CESG and others.[101] The numbers of GCHQ staff employed in the field of network defence and analysis of cyber attacks have increased by almost one-third in the last two years, significantly bolstering this critical aspect of cyber security work which currently accounts for over half of GCHQ's total cyber effort. Describing GCHQ's monitoring capabilities, the Director said:

> ***.[102]

109. We mentioned in our last Annual Report that Russia and China are suspected of carrying out the majority of electronic attacks. Such attacks are focused on espionage and acquisition of information. The Committee has been told that more work is required to understand the nature and extent of the threat from these and other countries.

110. While attacks in cyberspace represent a significant threat to the UK, and defending against them must be a priority, we believe that there are also significant opportunities for our intelligence and security Agencies and military which should be exploited in the interests of UK national security. In the Committee's view, these could include:

---

[101] *The Security Service also investigates state-sponsored cyber activity targeting the UK, in line with GCHQ's work.*
[102] *Oral Evidence – GCHQ, 1 March 2012.*

- *Active defence*: Interfering with the systems of those trying to hack into UK networks.
- *Exploitation*: Accessing the data or networks of targets to obtain intelligence or to cause an effect without being detected.
- *Disruption*: Accessing the networks or systems of others to hamper their activities or capabilities without detection (or at least without attribution). The most famous example of this type of cyber activity (although not involving the UK agencies) is the Stuxnet virus which is believed to have caused some disruption of the Iranian nuclear enrichment programme.
- *Information operations*: Using cyber techniques and capabilities in order to deliver information operations.
- *Military effects*: The destruction of data, networks or systems in support of armed conflict.

111. ***.[103]

112. GCHQ told us that work to protect UK interests in cyberspace has increased significantly in recent years but more still needs to be done:

***.[104]

M. Twenty months into the National Cyber Security Programme, there appears to have been some progress on developing cyber capabilities. However, cyber security is a fast-paced field and delays in developing our capabilities give our enemies the advantage. We are therefore concerned that much of the work to protect UK interests in cyberspace is still at an early stage.

[103] *Oral Evidence – Foreign Secretary, 26 January 2012.*
[104] *Oral Evidence – GCHQ, 1 December 2012.*

ACCESS TO COMMUNICATIONS DATA

113. The right of citizens to go about their business without interference from the state is an important principle of our way of life. Article 8 of the European Convention on Human Rights (ECHR) states that "*everyone has the right to respect for his private and family life, his home and his correspondence*", and that:

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*[105]

114. The intelligence and security Agencies, the police, law enforcement organisations and other public bodies already have powers, which are compliant with the ECHR, to monitor the activities of individual citizens. These are set out and controlled by the Regulation of Investigatory Powers Act 2000 (RIPA).[106] Broadly speaking, the powers can be divided into two categories:

- Intrusive: These represent the most serious invasions of a person's privacy, and include intercepting the contents of a communication (phone calls, emails or post), placing a listening device in a car or property, or installing surveillance devices on private property. All interception and property interference by the intelligence and security Agencies requires prior approval by the Secretary of State.[107]

- Non-intrusive: This is a less severe incursion on someone's privacy, and may include gathering data about someone's communications activity (e.g. establishing that one telephone number contacted another, but *not* the content of that call or text message), or surveillance of an individual in a public place. Authorisations for these can be given by a senior police or intelligence officer.[108]

115. As well as setting out the nature of the powers, RIPA also put in place a framework detailing which bodies could access these powers, under what circumstances, and who had the authority to permit the activity.[109] RIPA further established a number of Commissioners whose role is to oversee the use of these powers and ensure that they are being discharged legally. Each of the Commissioners – who are usually senior High Court judges – carries out inspections of the agencies or bodies within their remit to ensure that the RIPA powers are not being misused. They then each present a report annually to the Prime Minister on their findings (these reports are publicly available). In the case of communications, it is the Interception of Communications Commissioner who performs this function.[110]

---

[105] *European Convention on Human Rights, pp 10–11.*

[106] *Regulation of Investigatory Powers Act 2000, c 23.*

[107] *Approval for intrusive surveillance and property interference by law enforcement can also be granted by an independent Surveillance Commissioner (an ex-High Court judge or Appeals Court judge appointed by the Prime Minister).*

[108] *Depending on the nature of the information or activity being requested, authorisations can only be granted by someone at Inspector or Superintendent level or above (or the equivalent grade in the Agencies).*

[109] *RIPA has sometimes been criticised for allowing bodies such as local authorities access to powers that are considered disproportionate to the offences they are investigating (e.g. dog-fouling or fly-tipping). We do not cover this aspect of RIPA here, but instead concentrate on the intelligence and security Agencies and police and law enforcement when investigating terrorism or serious criminal offences.*

[110] *Currently the Rt. Hon. Sir Paul Kennedy.*

Current powers to access communications data

116. Under Part 1, Chapter 2 of RIPA, the police and intelligence and security Agencies currently apply to Communication Service Providers (CSPs) for details such as the registered subscriber of a telephone or email address, itemised billing of a telephone number, the location details of a mobile phone at a particular time and top-up details for pre-pay mobile phones. None of this reveals the content of any communication. Such requests are normally retrospective – communications data is rarely tracked in real time. Aside from situations where there is an immediate 'threat to life' (such as a live kidnapping), it could take up to several weeks between an officer deciding to apply for such information, for the authorisation to be given by a senior official, and the CSP then to provide a response. It is also important to note that this information is not held by government, but by the CSPs themselves.[111]

117. According to the Interception of Communications Commissioner, over 500,000 requests for communications data were made in 2010 under Part 1, Chapter 2 of RIPA.[112] This type of information is crucial to the work of the Agencies and the police. It is regularly provided to an evidential standard and used in court to support prosecutions:[113] communications data was successfully used to prosecute Ian Huntley for the Soham murders and in the trial of the Operation CREVICE 'fertiliser bomb' plotters. We have been told that every major Security Service investigation in the past decade and 95% of serious organised crime investigations have relied on communications data.[114]

Why change may be necessary

118. The changes in the telecommunications industry, and the methods being used by people to communicate, have resulted in the erosion of the ability of the police and Agencies to access the information they require to conduct their investigations. Historically, prior to the introduction of mobile telephones, the police and Agencies could access (via CSPs, when appropriately authorised) the communications data they required, which was carried exclusively across the fixed-line telephone network. With the move to mobile and now internet-based telephony, this access has declined: the Home Office has estimated that, at present, the police and Agencies can access only 75% of the communications data that they would wish, and it is predicted that this will significantly decline over the next few years if no action is taken. Clearly, this is of concern to the police and intelligence and security Agencies as it could significantly impact their ability to investigate the most serious of criminal offences.

---

[111] *CSPs are bound under European Union law to retain certain data and make it available when requested.*
[112] *HC 1239.*
[113] *Written Evidence – Home Office, 12 March 2012.*
[114] *Written Evidence – Home Office, 23 February 2012.*

Reduction in the ability to access data

- Data retention legislation[115] pre-dates the significant growth of the internet over the past decade. CSPs are not legally obliged to retain certain communications data such as every internet site visited (in the same way as calls made and received are logged).
- The rise in popularity of social networking and instant messaging has introduced new methods of communication (e.g. BlackBerry Messenger, which was used by many involved in organising the August 2011 riots). Many of these internet-based tools are based outside the UK, and the companies running them have no business or legal requirement to retain detailed records of communications made. UK-based CSPs who carry this traffic to domestic customers are also not legally obliged to retain any records of this data.
- As CSPs have moved towards offering tariffs with unlimited calls, texts and data use, there is less business need to hold records of how an individual uses these benefits.

N. The transition to internet-based communication, and the emergence of social networking and instant messaging, have transformed the way people communicate. The current legislative framework – which already allows the police and intelligence and security Agencies to access this material under tightly defined circumstances – does not cover these new forms of communication.

The Government's proposals

119. The Communications Capabilities Development (CCD) Programme, run by the Office for Security and Counter-Terrorism in the Home Office, was established to find a solution to this problem, and to ensure that the police and Agencies continue to have access to the communications data they require for their investigations.[116]

120. On 14 June 2012, the Home Secretary published a draft Bill setting out how the Government would revise powers to access communications data. The Home Secretary said:

> *Communications data saves lives. It is a vital tool for the police to catch criminals and to protect children. If we stand by as technology changes we will leave police officers fighting crime with one hand tied behind their backs.*
>
> *Checking communication records, not content, is a crucial part of day-to-day policing and the fingerprinting of the modern age – we are determined to ensure its continued availability in cracking down on crime.*[117]

121. The draft Bill will be subject to pre-legislative scrutiny by a Joint Committee of both Houses of Parliament. The Intelligence and Security Committee will also be conducting an Inquiry, focusing on the impact of the Bill on the intelligence and security Agencies. We intend to report our findings later in the year.

---

[115] *The Data Retention (EC Directive) Regulations 2009 transposed the EU Data Retention Directive – which is the primary basis for data retention across the EU – into UK law.*

[116] *Other strands of the CCD programme focus on implementing a single IT system to streamline requests to, and responses from, CSPs, and increasing awareness and understanding in the police and Agencies of how the new areas of data can contribute to investigations.*

[117] *www.homeoffice.gov.uk/media-centre/news/communications-data-bill.html*

COUNTER-PROLIFERATION

122. The UK's National Security Strategy[118] identifies an attack on the UK, including the use of Chemical, Biological, Radiological or Nuclear (CBRN) weapons, to be a Tier Two risk – this takes into account both the probability and consequences of such an event.[119] The UK continues to engage in international efforts to prevent the proliferation of Weapons of Mass Destruction.

123. In March 2012 the UK launched a new National Counter Proliferation Strategy[120] prior to the international Nuclear Security Summit in South Korea from 26 to 28 March. The strategy has three objectives:

i. to deny terrorists the materials to make and use nuclear weapons;

ii. to stop countries such as Iran and North Korea from obtaining or proliferating Weapons of Mass Destruction or advanced conventional weapons; and

iii. to build up the International Atomic Energy Authority (IAEA), UN and other organisations and treaties which help the UK to meet its goals through the international community.

A joint communiqué at the end of the summit reaffirmed a commitment to nuclear disarmament, non-proliferation and the promotion of peaceful uses of nuclear energy. It noted that "*nuclear terrorism continues to be one of the most challenging threats to international security*".[121]

124. The three intelligence and security Agencies devote varying levels of resource to Counter-Proliferation work. SIS and GCHQ undertake the bulk of the work (***% and ***% of their overall allocation of effort respectively), whereas the Security Service has a more limited contribution focusing on disrupting attempts to procure prohibited items from within the UK.

125. A new addition this year is a 'virtual hub' within Defence Intelligence (DI) "*for counter-proliferation technical assessment… which … join[s] up proliferation expertise from across the community and wider government*".[122] This was established as a result of the 2010 Strategic Defence and Security Review, and is now fully operational. We have been told that "*initial signs are that it is working well*".[123] Its work focuses on "*monitoring the weapons of mass destruction programmes and capabilities of a number of states of concern and of the impact of counter-proliferation regimes and treaties designed to restrict these programmes*".[124]

---

[118] *Cm 7953.*
[119] *International terrorism and hostile attacks on UK cyberspace are considered Tier One risks.*
[120] *www.fco.gov.uk/resources/en/pdf/global-issues/weapons-proliferation/counter-proliferation-strat*
[121] *www.thenuclearsecuritysummit.org/userfiles/Seoul%20Communique_FINAL.pdf*
[122] *Cm 7948.*
[123] *Written Evidence – Defence Intelligence, 28 September 2011.*
[124] *Ibid.*

Iranian nuclear programme

126. The prospect of the Iranian regime acquiring nuclear weapons capability remains a serious concern, and preventing this is a key strand of the Government's Counter-Proliferation strategy. In November 2011, the IAEA published a report stating that Iran continues to undertake activities to acquire such capability. It said:

- it is concerned about the possible existence in Iran of undisclosed nuclear-related activities involving military-related organisations, including activities related to the development of a nuclear payload for a missile;
- it has serious concerns regarding possible military dimensions to Iran's nuclear programme; and
- Iran has, in the past, carried out activities relevant to the development of a nuclear explosive device and that some of these activities may still be ongoing.[125]

127. The Government believes that if Iran were to acquire nuclear weapons capability, other states in the region would feel under pressure to follow. This would lead to an inherently unstable Middle East and would threaten global energy security. In addition, the Israeli Government has threatened to take unilateral military action against the Iranian nuclear programme, and Prime Minister Netanyahu has said he will not tolerate a long delay in launching an attack on Iran's nuclear sites: "*We've waited for diplomacy to work. We've waited for sanctions to work. None of us can afford to wait much longer*."[126] The issue is thus one of the most serious crises in foreign policy that the international community currently faces.

128. The past two years have seen a series of deaths of Iranian nuclear scientists in explosions inside Iran, with four being killed since 2010. There have also been reports of explosions at several Iranian facilities that have connections with its nuclear programme. We have been told that only one of the reported explosions could be verified, and this was assessed as having been an accident, probably caused by inadequate safety procedures being applied. The Chief of SIS said:

> *There has been quite a lot of information about the explosions in Iran. The one which we are clear took place was at the missile centre to the west of Tehran, where there was a major explosion, the causes of which are not entirely clear, but it's likely it was an accident… and their handling procedures did not seem to be of the standards that we would expect from any western country, and it could well be that it was an accident and that is the most likely explanation.*[127]

129. The Israeli intelligence services are widely alleged to have been responsible for at least some of these attacks. Israeli interests have been targeted in Georgia, Thailand and India, possibly in retaliation. The Foreign Secretary stressed to us that the UK was not involved in the assassination of nuclear scientists, a point repeated by the Chief of SIS.

---

[125] *'Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran', 8 November 2011.*

[126] *Prime Minister Netanyahu's speech to the American Israel Public Affairs Committee (AIPAC), 5 March 2012.*

[127] *Oral Evidence – SIS, 15 December 2011.*

The UK Government's response

130. The UK's response has been to work with its international partners in an effort to persuade Iran to enter negotiations that would demonstrate that it is not developing nuclear weapons. This has two elements:

i. diplomacy and engagement with Iran; and

ii. pressure on Iran in the form of peaceful and legitimate sanctions.

131. In our 2010–2011 Annual Report, we noted that it appeared that the combined effect of sanctions and the work of the intelligence and security Agencies has been to delay the progress of the Iranian nuclear programme.[128] We asked for an update this year, and were told by the Foreign Secretary:

> *I think that [the UK] has undoubtedly made some contribution, and we are not the only country that does that, ***.*
>
> *I have no doubt that the strength of our response to the Iranian programme diplomatically and in terms of sanctions does help… [but our actions are] not a strategic success because the Iranian nuclear programme continues.*[129]

132. The Foreign Secretary went on to confirm that in addition to its diplomatic efforts, the UK intelligence and security Agencies and others have been working together to try to limit Iran's procurement of material. In addition, SIS told us that it has ***.[130]

133. DI told us that it had:

> ***.[131]

134. UK–Iranian relations have deteriorated over the past 12 months, with Iran taking hostile action against UK interests. In November 2011, the British Embassy in Tehran was attacked and destroyed by a crowd of protestors. All the Embassy personnel had to be evacuated and Embassy property secured. The British Ambassador to Iran later stated that the attack must have had the backing of the Iranian regime. In response, the Government expelled Iranian diplomatic personnel from the UK. In March 2012, the UK's Foreign and Commonwealth Office web pages on Iran were blocked within the country by Iranian censors.

O. The prospect of Iran acquiring nuclear weapons is of serious concern. The UK must continue, with our international partners, to apply diplomatic and economic pressure to persuade the Iranian regime to alter its course. We support the Government's efforts, and those of the Agencies, whose work against this threat is invaluable.

---

[128] *Cm 8114.*
[129] *Oral Evidence – Foreign Secretary, 26 January 2012.*
[130] *Oral Evidence – SIS, 15 December 2011.*
[131] *Oral Evidence – Defence Intelligence, 8 March 2012.*

INTERNATIONAL CO-OPERATION

Working with foreign intelligence services

135. Previous sections of this Report have illustrated the international nature of the threat facing the UK. It would be difficult, if not impossible, for our Agencies to confront such threats if they worked in isolation; to protect our national security they depend on intelligence shared with us by our foreign partners. Since 2001, the necessity of such international co-operation has been widely recognised; indeed, all UN member states are bound by Security Council Resolution 1373 to share intelligence and co-operate with each other to prevent terrorist attacks.[132]

136. The nature of the current international terrorist threat means that the Agencies have to work closely with their counterparts in the Middle East and the Arabian Peninsula, North Africa and the Maghreb, and South, Central and East Asia. Such close co-operation with countries that may take a different view, or operate to different standards, when it comes to human rights and treatment of detainees gives rise to moral and ethical problems.

137. Following the investigation by the Committee in the last Parliament into the case of the former Guantánamo Bay detainee, Binyam Mohamed, the ISC urged the then Prime Minister to make clear publicly the difficulties faced in dealing with foreign intelligence agencies, and also recommended that the Agencies be given clear guidance in such circumstances:

> *… the key issue raised in the Binyam Mohamed case is not new. How do we reconcile the need to obtain vital intelligence to protect the British public, with the need to ensure that an individual's human rights are not infringed? This is a fundamental policy question which must be answered… While not condoning, soliciting or encouraging torture or [cruel, inhuman or degrading treatment], the reality is that our Agencies are required to take action which runs the risk of it happening – this is something we would hope to see expressed in any policy statement on this matter.* [133]

138. The joint article by the then Foreign and Home Secretaries in August 2009, which sought to explain that the risk of mistreatment cannot be completely eliminated if we have any intention of protecting UK citizens from attack, was a helpful contribution to the public debate. The article said:

> *When detainees are held by our police or Armed Forces we can be sure how they are treated. By definition, we cannot have that same level of assurance when they are held by foreign governments, whose obligations may differ from our own.*
>
> *Yet intelligence from overseas is critical to our success in stopping terrorism. All the most serious plots and attacks in the UK in this decade have had significant links abroad. Our Agencies must work with their equivalents overseas. So we have to work hard to ensure that we do not collude in torture or mistreatment.*
>
> *… our Agencies are required to seek to minimise, and where possible avoid, the risk of mistreatment. Enormous effort goes into assessing the risks in each case.*

---

[132] *United Nations Security Council Resolution 1373, approved and published 28 September 2001.*

[133] *Letter from the Chairman of the Intelligence and Security Committee to the Prime Minister, 23 April 2009.*

Operations have been halted where the risk of mistreatment was too high. But it is not possible to eradicate all risk. Judgments need to be made.[134]

139. Furthermore, when the current Government published the 'Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees' in July 2010, the Prime Minister said in a statement to the House:

> *… [the guidance] makes clear the following: first, our services must never take any action where they know or believe that torture will occur; secondly if they become aware of abuses by other countries, they should report it to the UK Government so we can try to stop it; and thirdly, in cases where our services believe that there may be information crucial to saving lives but where there may also be a serious risk of mistreatment, it is for Ministers, rightly, to determine the action, if any, that our services should take.*[135]

P. The UK does not condone, solicit or encourage torture or cruel, inhuman or degrading treatment (CIDT). However, to protect the UK our Agencies must work with foreign agencies, some of whom do not meet our standards. In so doing, there is a risk that our Agencies will, indirectly and inadvertently, be linked to such activities. It is unfortunate, but inescapable, that those risks cannot always be wholly eliminated. The challenge therefore is how to minimise that risk, while maintaining essential intelligence-sharing relationships with our international partners.

The Detainee Inquiry

140. Such difficulties lie at the heart of the questions around UK complicity in the rendition, torture or cruel, inhuman and degrading treatment (CIDT) of detainees. On 6 July 2010, the Prime Minister announced plans to address these concerns, including a judge-led Inquiry, headed by Sir Peter Gibson. The Inquiry was due to start once police investigations into allegations of UK involvement in the mistreatment of two individuals, Binyam Mohamed and another detainee held by the US in Afghanistan, were concluded.[136]

141. In January 2012 the Crown Prosecution Service and the Metropolitan Police Service announced that no charges would be brought in either case. However, following further allegations relating to UK involvement in rendition operations to Libya, the police launched a new investigation into these cases. As a result, the Justice Secretary told Parliament on 18 January 2012:

> *These further police investigations into the Libyan allegations may take some considerable time to conclude. The Government fully intends to hold a judge-led inquiry into these issues once it is possible to do so and all related police investigations have been concluded. There now appears to be no prospect of the Gibson Inquiry being able to start in the foreseeable future. So, following consultation with Sir Peter Gibson, the chair of the Inquiry, we have decided to bring the work of his Inquiry to a conclusion.*[137]

---

[134] *"We firmly oppose torture – but it is impossible to eradicate all risk", Foreign Secretary and Home Secretary – joint article for the Sunday Telegraph, 8 August 2009.*

[135] *HC Deb, 6 July 2010; vol. 513 col. 177.*

[136] *These investigations (Operation Hinton and Operation Iden) sought to establish whether or not criminal charges should be brought against individual officers within the intelligence and security Agencies.*

[137] *HC Deb, 18 January 2012; vol. 538 col. 752.*

Q. The Committee understands the reasons for halting the current Detainee Inquiry and supports the Government's plans to hold another judge-led inquiry when possible. The specific allegations of UK involvement in renditions of two individuals to Libya remain under police investigation and we will, therefore, not be commenting further at this time.

Libya

142. The new police investigation concerns allegations that came to light following the collapse of the Gaddafi regime, when a number of intelligence files were discovered in the abandoned offices of former Foreign Minister, and ex-head of the Libyan External Security Organisation (ESO), Musa Kusa. It is alleged that these papers show that SIS co-operated with ESO in the rendition of Sami al-Saadi and Abdul Hakim Belhaj.

143. Given the seriousness of these allegations, we began an Inquiry into the allegations and also wider questions surrounding the UK's intelligence relationship with Libya. However, when the police began their investigation, we had to suspend our Inquiry (for the same reason that the Detainee Inquiry was halted) and cannot, therefore, comment further at this time. We will resume our own Inquiry as soon as we are able to do so.

REFORM OF THE INTELLIGENCE COMMUNITY

Protecting intelligence in the courts

The Justice and Security Green Paper

144. The Government published the Justice and Security Green Paper on 19 October 2011.[138] The Green Paper outlined potential reforms concerning the handling of sensitive material in civil cases (it did not affect procedures in criminal cases). It said:

> *The civil courts… have heard increasing numbers of cases challenging Government decisions and actions in the national security sphere. By their very nature such cases involve information which, under current rules, cannot be disclosed in a courtroom… This information must be protected appropriately, as failure to do so may compromise investigations, endanger lives and ultimately diminish our ability to keep the country safe… [The] Green Paper aims to respond to the challenges of how sensitive information is treated in the full range of civil proceedings… It seeks to find solutions that improve the current arrangements while upholding the Government's commitment to the rule of law. We urgently need a framework which will enable the courts to consider material which is too sensitive to be disclosed in open court.*[139]

Closed material procedures in civil proceedings

145. The Green Paper proposed that where highly sensitive material is concerned, proceedings should include both open and closed elements rather than taking place entirely in an open court.[140] This is counter-intuitive, given the UK's long tradition of open justice, but given that the alternative is putting the UK and its citizens in harm's way, it is justified – in certain clearly defined circumstances and with safeguards. It is also important to note that these reforms apply only to civil proceedings: there are no changes proposed to criminal proceedings where an individual's liberty might be at stake.

146. The Committee considers it preferable that such cases are considered in proceedings that include closed elements rather than not at all. We have seen recent cases involving our intelligence and security Agencies run into difficulty, given the sensitivity of some of the material relevant to the case, with the Government forced to abandon its defence of civil cases and settle out of court rather than risk highly sensitive material becoming public. This does not therefore result in a fair trial.

147. The current arrangement for protecting such highly sensitive material from public disclosure – the Public Interest Immunity (PII) system – does not result in a fair trial either. PII allows such material to be excluded from judicial proceedings (where the public interest so demands). However, this means that not all the relevant information is available – to either party. This is to the detriment of at least one if not both parties, and justice cannot therefore be said to be done.

148. Abandoning cases or withholding relevant material from the judge is not to see justice done at all: those who argue against closed proceedings and for using PII for such material are, paradoxically, arguing for a less open and fair system.

---

[138] *Cm 8194.*

[139] *Ibid.*

[140] *This is already the case in certain immigration and other proceedings, and the Green Paper proposed extending this to civil proceedings.*

The scope of material to be protected

149. Nevertheless, the scope of the material to be protected in this way is key, and this is where the Committee considered that the Green Paper did not offer sufficient clarity. The safety of the British public will, in very special cases, provide justification for altering the usual trial procedures. However, the Committee argued that the material to be protected must be such that it really would jeopardise the national security of the UK if it were to be made public. These special arrangements, therefore, must be the exception, not the rule, and the provisions must not be abused.

150. Not all sensitive material warrants such special treatment. For example, the Green Paper mentioned diplomatic exchanges and there were suggestions that 'the public interest', rather than national security, should be the determining factor in deciding whether closed material procedures (CMPs) should be ordered. This was too broad by far – we argued that the Committee could not support such a broad definition of 'sensitive information'. The Committee was clear that the special arrangements should not be used to avoid difficult or embarrassing situations. Nor should material be excluded simply because it is labelled as 'secret'.

151. There are only two narrow categories of information which can rightly be said to be that sensitive:

- The first is UK intelligence material which would, if disclosed publicly, reveal the identity of UK intelligence officers or their sources, and their capability (including the techniques and methodology that they use);
- The second is foreign intelligence material, provided by another country on a strict promise of confidentiality.

152. The first category is easily understood: we must not endanger the lives of those who work – in very dangerous situations – to protect us, nor must we reveal how they foil terrorist plots, or their ability to detect and disrupt future plots will be reduced. We believe that the public expects such information to be protected. (Whilst intelligence officers' identities must be protected, this would not preclude them giving evidence in open proceedings – on less sensitive information – and on grounds of anonymity.)

153. The second category is more often misunderstood. The current threat from international terrorism requires an international response. Our Agencies cannot work in isolation: many of the most serious plots and attacks in the UK in the last decade have had significant links abroad and therefore we must make use of foreign intelligence partnerships in order to safeguard our security and prevent terrorist attacks.

154. Understandably other countries want to know that the UK can be trusted with their intelligence material. In this respect, whilst UK Agencies are given foreign intelligence material by those with whom they co-operate, it does not then belong to us and is not ours to do with as we wish. It is not therefore up to the UK to decide who else we might share it with – that decision rests with the country that 'owns' the material. This principle is sacrosanct, and we must not break it. Put simply, if the UK Agencies break that 'control principle', foreign intelligence agencies will not trust us to protect any of their intelligence material and therefore will not share as much intelligence material with our Agencies. The

lack of that foreign intelligence material could put the UK in serious danger, given the amount of information on plots to harm the UK that comes from foreign intelligence.

155. There are those who refuse to believe either that such a principle exists, or that breaking it would have any serious repercussions. All we can say is that they do not know – understandably given that this is a secret world – what they are talking about. We speak regularly with those who share intelligence material with the UK. We know how seriously the 'control principle' is treated and just how damaging it would be for the UK to break its word.

156. It is also important to understand that this principle applies to all foreign intelligence material, whether sensitive or not. For example, the foreign intelligence material in the Binyam Mohamed case was not highly sensitive, and indeed to a certain extent was already in the public domain. However, this misses the point. The overriding principle was that the UK Agencies did not 'own' the material and therefore were obliged to seek the permission of the originating nation, in this case the US, before disclosing it. The US refused to grant permission for public disclosure of its material in an open court judgment.

157. The courts did not accept this principle in the Binyam Mohamed case and the result has been that the US has re-examined some elements of its bilateral intelligence-sharing procedures. The Intelligence and Security Committee has heard some of the US's concerns first hand and is in no doubt that there has been an impact on intelligence co-operation. It is essential that the UK can be trusted: our Agencies must be able to give their word that they will not reveal intelligence material that our foreign partners have shared with us, or we will be shut out.

The protection offered

158. Whilst the scope of material to be protected must be limited to the two categories outlined above, it was equally important to the Committee that the protection was effective. The use of CMPs and Special Advocates would increase the protection which could be given to foreign intelligence material, but we were concerned that they may not offer sufficient reassurance to our allies. This lack of a guarantee was acknowledged in the Green Paper itself, which stated that CMPs would only "*reduce the risk of damaging disclosure of sensitive material*".[141]

159. We spoke to the Agencies about the proposals in the Green Paper. The Director of GCHQ said that: "*I think the Green Paper has been a hugely positive construct.*"[142] This sentiment was echoed by the Director General of the Security Service, who said:

> *I think it is the right direction and I think it will give a lot more comfort. I am sure the Americans will still want to press for as much protection as they can, but I think in all the circumstances, this is a very good way forward… I think that given the fact that… it will be in individual cases that this gets tested, we are more likely to have a successful outcome if there is, broadly speaking, judicial support for the approach taken. Because otherwise, they will strain every sinew to get to a position which they feel… gives due weight to their own prerogatives.*[143]

---

[141] *Cm 8194.*
[142] *Oral Evidence – GCHQ, 1 December 2011.*
[143] *Oral Evidence – Security Service, 24 November 2011.*

160. The Chief of SIS made clear that some of our allies had very serious concerns about UK courts being used to obtain foreign intelligence under the 'Norwich Pharmacal' principle.[144] This allows a person with a complaint about the conduct of a foreign intelligence service to obtain sensitive material held by the UK Agencies, even where there is no complaint against the UK Agencies themselves: "*Norwich Pharmacal… remains actually the highest concern of the United States in this area…*"[145]

161. The Committee was concerned that the proposals did not go far enough in terms of our ability to protect foreign intelligence material. We therefore proposed in our response to the Green Paper that there should be a statutory presumption against disclosure of intelligence material. This would have the advantage of providing a clear indication to judges of Parliament's intention in relation to such material. We consider that judges themselves would welcome such clarity: the courts are usually interested as to whether they can infer Parliament's intentions from the wording of an Act. Such a presumption would be invaluable in this respect. Any presumption would, of course, be rebuttable and therefore the final decision would still lie with the courts, although there would need to be compelling reasons for a judge to rule against.

The Justice and Security Bill

162. Following a period of consultation on the Green Paper, on 28 May 2012 the Government introduced legislation to reform the procedures for handling sensitive information in civil proceedings (including 'Norwich Pharmacal' cases).

163. The Committee notes that the Government has narrowed the scope of those cases where CMPs can be invoked, and the process whereby this can take place. The Bill refers only to CMPs being used in cases where disclosure of material would be "*damaging to the interests of national security*".[146] This is an improvement over the original language of the Green Paper, which proposed that a much broader category of 'sensitive' material might be excluded merely on the grounds of 'public interest'. In addition, it is now judges who will have the final decision on whether the request by Ministers for a case (or part of a case) to be held under CMP conditions should be granted.

164. The Committee's initial response is broadly supportive. However, we will now need to subject the proposals to more detailed scrutiny as the Bill proceeds through Parliament.

Intelligence and Security Committee

165. In our last Annual Report we said that we had provided proposals to the Prime Minister as to how this Committee could be strengthened and, in particular, how to provide greater openness and transparency, and reassurance to the public and Parliament. These proposals were reflected in the Justice and Security Green Paper: the Government recognised that if there is to be greater protection for matters of national security in terms of judicial scrutiny, then it must be balanced by greater oversight of such matters through other bodies, and primarily this Committee.

---

[144] *A Norwich Pharmacal action is an equitable remedy developed by the courts in England and Wales, with an equivalent jurisdiction in Northern Ireland, requiring a respondent to disclose certain documents or information to the applicant. The respondent must be either involved or mixed up in wrongdoing by others, whether innocently or not, and is unlikely to be party to the potential proceedings. An order will only be granted where 'necessary' in the interests of justice. Orders are commonly used to identify the proper defendant to an action or to obtain information to plead a claim.*

[145] *Oral Evidence – SIS, 15 December 2011.*

[146] *HL Bill 27.*

Proposals regarding the ISC in the Green Paper

- *The Government has considered the ISC's own proposal that it becomes a statutory Committee of Parliament alongside its existing reporting arrangements to the Prime Minister. The Government proposes that this option is pursued.*
- *The Government is giving careful consideration to the ISC's proposal to extend its remit to include operational aspects of the work of the Agencies. Any such oversight of operational work would need to be clearly retrospective and in the Government's view would need to be focused on matters of significant national interest. Any change of this kind would therefore need to be based on a clear understanding between the Government and the Committee on how this should work in practice, articulated either in legislation or, possibly, a supporting document such as a Memorandum of Understanding.*
- *The Government proposes formally to recognise the wider role the ISC should play in overseeing the Government's intelligence activities by enabling it to take evidence from any department or body in the wider intelligence community.*
- *The Government has looked at whether additional reforms could be made to further normalise ISC appointments.*
- *The Government is considering possible changes to the ISC's staffing, accommodation and funding with a view to strengthening both the ISC's actual and symbolic connection to Parliament.*
- *The Government proposes to review the level of resourcing that the ISC requires to support it in the discharge of its functions and the nature of the skills the Committee requires to have at its disposal.*
- *The Government is committed to work with the ISC to provide public evidence sessions where this can be achieved without compromising national security or the safety of individuals.*
- *The Government agreed with the ISC's proposal that the Committee should be given the power to require information from the intelligence Agencies. The Government also agrees with the ISC proposal that this should be subject only to a veto exercisable by the relevant Secretary of State, rather than by the Head of the individual Agency, as now.*[147]

166. The Committee welcomed the Government's proposals. However, there were three aspects on which we sought further clarification:

i. the division of responsibilities between this Committee and the two Commissioners;

ii. the extent of oversight of operations; and

iii. the provision of additional resources to support the extended remit.

[147] *Cm 8194.*

The Committee and the Commissioners

167. The work of the Commissioners, assisting Ministers by providing a compliance, audit and assurance function, is vital. However, the Green Paper proposed that their duties should be expanded to include "*adding a general responsibility for overseeing the effectiveness of operational policies to the statutory remit of the Intelligence Services Commissioner*".[148] The Committee was concerned that this represented a blurring of boundaries. It is the Commissioners' function to monitor compliance with legislation, rules and procedures. This is a quasi-judicial role, the purpose of which is to reassure Ministers, Parliament and the public that the rules governing the covert and intrusive work of the Agencies are being complied with. The Commissioners also provide advice to the Agencies to develop better rules, procedures and guidance, in order to improve compliance over time. General responsibility for oversight of the appropriateness and effectiveness of policy, including policy which impacts on the operational work of the Agencies, is the remit of the Intelligence and Security Committee. We proposed, in our response to the Green Paper, that this should not change, nor should it be a shared responsibility between the Committee and the Commissioners, since this would risk confusion and duplication.

168. We note that the Bill, as introduced, provides for the Intelligence Services Commissioner to be directed by the Prime Minister to "*keep under review the carrying out of any aspect of the functions of [the intelligence services]*".[149] The Bill explains that this could include reviewing "*the implementation or effectiveness of particular policies of the head of an intelligence service regarding the carrying out of any of the functions of the intelligence service.*"[150] The Committee remains concerned that, although the Government's intention may be to maintain a clear separation, the potential for duplication or overlap between the Commissioner's proposed role in considering the "*effectiveness of particular policies*" and the ISC's remit to provide oversight of policy more generally remains. We will be seeking further information and reassurance from the Government on this point.

Oversight of operations

169. The ISC has for many years reported on operations, both publicly and in confidence to the Prime Minister. This includes reports as far back as the 1999 Inquiries into Sierra Leone and the Mitrokhin Archives, when the Committee was still relatively new, through to more recent examples such as the 2007 Inquiry into the 7/7 bombings and the 2009 Inquiry into the Binyam Mohamed case. Some of these investigations were at the express request of the Prime Minister; others were instigated by the Committee itself. They were all specific operations that gave rise to public concern and significant national interest, and they were all Inquiries in which the Committee had access to specific, detailed, operational material. The Committee considered that the current arrangements should be formalised and this work placed on a statutory footing. Moreover, given that the ISC has already had substantial oversight of operations, we argued that any reforms should not restrict the Committee's responsibility merely to policy, resources and administration as in the 1994 Act.

---

[148] *Ibid.*
[149] *HL Bill 27.*
[150] *Ibid.*

170. In our discussions prior to the publication of the Green Paper, we were mindful of the Government's concerns in this area. To that end, we proposed that the Committee's Inquiries would be retrospective and that they would be limited to matters of significant public interest. Even so, the wording in the Green Paper remained rather circumspect, stating only that "*the Government is giving careful consideration to the ISC's proposal to extend its remit to include operational aspects of the work of the Agencies*".[151]

171. We were therefore pleased that the Bill makes specific reference to the ISC having the power to oversee the operations of the intelligence and security Agencies, subject to this power being retrospective and in relation to matters of significant national interest. This is consistent with the role the ISC has developed since its inception, and formalising this is a sensible recognition of the current practice.

Resourcing

172. The proposed changes to the Committee's powers and remit will involve new ways of working. The key difference will be as a result of the Committee's power to 'require' information to be provided, subject only to a veto exercisable by the relevant Secretary of State. Whereas currently the Committee is reliant on the Agencies to decide what information to provide in response to our requests, this change will mean that it will be for the Committee, through its staff, to determine the information that we require. This will necessitate an increase in the number and seniority of the Committee's staff, with a proper investigative capacity with sufficient levels of access and powers. If we are to provide credible and effective oversight then we must be resourced to do so. This view is supported by comparisons with our counterparts in the US and Canada and by discussions with practitioners in the UK.

173. We were pleased that the Government has recognised that the Agency Heads should not have the power to veto the release of information to the Committee on national security grounds. It is appropriate that this power instead rests with the relevant Minister. While the greater powers and remit of the Committee are a significant and welcome change, the effective discharge of these functions will require increased levels of staff and investigative resources. We welcome the National Security Adviser's pledge to make early progress on this matter.[152]

Defence Intelligence

174. Defence Intelligence (DI) is part of the Ministry of Defence (MoD) and is mostly funded from within the MoD budget. DI provides strategic intelligence to inform MoD policy and procurement decisions and tactical and operational intelligence to support military operations overseas. However, large parts of its strategic analysis work also support wider government – and particularly the Joint Intelligence Committee – and so it has a national role to play alongside the three main intelligence and security Agencies. Indeed, DI has the largest pool of all-source analysts in government.

---

[151] *Cm 8194.*

[152] *Letter from the National Security Adviser, 19 March 2012.*

Reviews

175. 2011 saw two significant reviews which will impact on DI: firstly, the Government's review of the central intelligence machinery;[153] and secondly, the review of the MoD's central structure carried out by Lord Levene.[154]

176. The review of the central intelligence machinery was announced by the then Cabinet Secretary in January 2011, and its conclusions were reported to the Prime Minister in September 2011. Among other conclusions, the review recommended that "*the wider assessment capability, including Defence Intelligence and the Joint Terrorism Analysis Centre, should be put more directly at the disposal of the [National Security Council] where appropriate*", and that the Director of Central Intelligence Assessment in the Cabinet Office would be responsible for commissioning material from the wider analytical community to inform National Security Council (NSC) discussions, and for ensuring its quality.[155]

177. The Levene report, which was presented to the Defence Secretary in June 2011, aimed to make the MoD's central management more strategic and efficient, with more responsibility for delivery devolved down to the front-line military commands. One of the key recommendations was the creation of a new Joint Forces Command (JFC), which would bring together all the supporting areas that contribute to successful military operations (such as intelligence, training and logistics). The report recommended that the majority of DI be transferred into this new command, with only the all-source analytical function remaining in MoD Head Office. It also recommended that thought be given to downgrading the seniority of the post of Chief of Defence Intelligence (CDI).

178. We have subsequently been told that the MoD has rejected the proposal to split DI. Instead it will be moved in its entirety into the new JFC. In explaining this decision, CDI told us that:

> *… we felt that everything we know about the way we were going to operate in the future – and this is supported by the view of American colleagues, Australian colleagues, Canadian colleagues, so this isn't just an entirely British view – [pointed to] closer working between assessment and collection staff and, were you to split them off as two separate groupings, that would be inappropriate…*[156]

179. CDI also told us that he believed his post would retain its current level of seniority, particularly as it has had additional duties assigned to it. These include responsibility for MoD's cyber and counter-intelligence work, as well as oversight of MoD's 'information superiority' equipment programme.[157] However, he acknowledged that this issue "*remains open for review in 2013*".[158] CDI also told us that in the future it was possible that the post may become a civilian, rather than an exclusively military, position.

---

[153] *The central intelligence machinery refers to the Joint Intelligence Organisation and National Security Secretariats in the Cabinet Office and, in this context, the analytical functions of Defence Intelligence and the Joint Terrorism Analysis Centre (JTAC – a part of the Security Service).*

[154] *Defence Reform – An independent report into the structure and management of the Ministry of Defence, June 2011.*

[155] *www.cabinetoffice.gov.uk/resource-library/nscrecommendations*

[156] *Oral Evidence – Defence Intelligence, 8 March 2012.*

[157] *Ibid.*

[158] *Ibid.*

R. Defence Intelligence makes a critical contribution to the UK's intelligence collection and assessment capabilities. However, it is often not thought of as part of the central intelligence machinery and the Committee is concerned that its vital role sometimes goes unrecognised. We hope that the reforms will result in DI obtaining the profile its work deserves.

Support to operations

180. Supporting the military effort in Afghanistan remained DI's key priority in 2010/11. We heard last year about the creation of the Defence Intelligence Fusion Centre (Afghanistan) (DIFC(A)), which brings together all of DI's all-source analysis on Afghanistan regionally into one team. We asked for an update on the work it was producing. We were told:

> *… the sort of work that it's doing ranges from, at the strategic level, providing advice to the Government's special representative, Mark Sedwill, and also the NSC, on how we think the insurgency is likely to unfold over the next five to ten years… [at] the operational level, *** and then dropping down a level further… they are also bringing together information from across theatre… to try and understand better the [Taliban] networks.*[159]

181. At the operational level, we were also told ***.

182. While this work is encouraging, last year the Committee was told that there was a shortage of Human Intelligence (HUMINT) operators – despite an agreement from the MoD in 2009 to increase numbers – and that this was impacting on the counter-IED work. The delay was explained to us as being due to the long lead-in time for training new recruits and a shortage of instructors. This year we were told that numbers had increased, but CDI said that "*we [still] haven't got all of the extra staff now in place… it is not a trivial task to both recruit, to train and retain these people*".[160] The attrition rate for the courses that recruits must pass to be qualified to undertake such roles remains high; as it was put to us, "*we can get volunteers in through the door, but, actually, just getting people who can drive, read a map, shoot, listen to an earpiece and debrief somebody all at the same time is the difficult piece*".[161]

Defence Intelligence's response to the 'Arab Spring'

183. The reductions in analyst numbers over the last few years have meant that some of the lower-priority areas have seen a thinning out of resources, and this was the case for North Africa prior to the 'Arab Spring'. DI admits the countries involved "*had little resource directed to [them] until events in Tunisia in January 2011*".[162] When we questioned DI about this, we were assured that "*we are able to keep an eye on what's going on around the world [although] clearly we prioritise effort in those areas that matter most to UK national interests and defence*".[163] Where the situation demands it DI is "*able still to surge more people into areas when there's a national priority to do so*".[164] This is inevitably at the cost of other areas, and in the case of the 'Arab Spring' DI admitted that "*greater risk*

---

[159] *Ibid.*
[160] *Ibid.*
[161] *Ibid.*
[162] *Written Evidence – Defence Intelligence, 28 September 2011.*
[163] *Oral Evidence – Defence Intelligence, 8 March 2012.*
[164] *Ibid.*

was taken against… areas including the Balkans, former Soviet central Asian states and sub-Saharan Africa".[165] We were also told that, given the proliferation of open source material available to the modern analyst, "*we can't cover everything all the time in the modern world*".[166]

184. On a positive note, we also heard how DI's contribution to the Libya campaign had raised awareness of its analytical capabilities across Whitehall, with DI being represented at almost every meeting of the NSC on Libya. The National Security Adviser told us that DI "*has found a new profile and relevance*" as a result.[167] We were also told by DI that:

> *We were also finding ourselves, and have continued to find ourselves, getting access and getting into meetings and getting [involved] in issues that previously we'd had to ask to get involved in. So I think people have appreciated across government and across defence the benefit that we brought and we're now very much, for example, part of the core thinking on issues such as Syria [and] Iran, as we should be. But, as I said, we're not having to ask now, we're automatically part of the core group.*[168]

Staffing reductions

185. The Committee has been concerned for several years about the overall diminution of DI's coverage and capabilities, primarily as a result of cuts to the numbers of analytical staff. The 2010 Strategic Defence and Security Review set out further cuts to the MoD budget of 8% over the Spending Review period. As DI is largely funded from the MoD budget, we were told DI expected to take a share of these savings. We therefore concluded in our Annual Report last year that "*the prospect of further cuts… has potentially very serious long-term consequences for DI's ability to support military operations and for the UK intelligence community as a whole*".[169]

186. In May 2011, we were informed that the MoD intends to cut by 12% the funding it provides to DI by 2014/15. This will mean the loss of 450 military and civilian posts, with a further 128 military posts being converted to civilian roles. DI estimates that the loss in overall analytical capability will be less than 10%, although this is predicated on a reduction in requirements on Afghanistan following the planned withdrawal of combat troops by the end of 2014. The Committee has been told that "*reductions of this level will have an impact on the organisation's ability to deliver the same level of output as currently*". We note also that the cuts may require specialist intelligence staff to take on more administrative duties, due to a loss of support roles.

S. Defence Intelligence has told us that it "*can't cover everything all the time in the modern world*". Nevertheless, Strategic Defence and Security Review cuts will further decrease DI's ability to provide global coverage with sufficient depth. It is therefore likely that even greater risk will have to be taken when reacting to the next crisis than was the case with the Libya campaign. This is an unsatisfactory position. We urge the Government to ensure that sufficient resources are available to allow in-depth coverage to be maintained on an ongoing basis.

---

[165] *Written Evidence – Defence Intelligence, 28 September 2011.*
[166] *Oral Evidence – Defence Intelligence, 8 March 2012.*
[167] *Oral Evidence – National Security Adviser, 20 October 2011.*
[168] *Oral Evidence – Defence Intelligence, 8 March 2012.*
[169] *Cm 8114.*

National Crime Agency

187. The lead for work against serious and organised crime in the UK currently lies with the Serious Organised Crime Agency (SOCA), working in close partnership with local police forces, other law enforcement agencies, the intelligence community and the devolved administrations. When SOCA was established in 2006, the intelligence community reduced the effort they devoted to organised crime. The Security Service ceased work in this field altogether; however, SIS and GCHQ still provide support to SOCA, gathering intelligence on criminal groups and conducting joint operations to disrupt their activity overseas.

188. In its 2010 Policing and Justice White Paper, the Government said that the fight against organised crime was fragmented across too many individual agencies to be effective, and lacked cross-government strategy and a national tasking and co-ordination mechanism. It therefore proposed the establishment of a new National Crime Agency (NCA), alongside directly elected Police and Crime Commissioners. On 11 May 2012, the Crime and Courts Bill was introduced into Parliament: this will provide the legislative basis for the NCA, which will replace SOCA. The NCA is due to launch in 2013.

189. Current plans envisage four 'commands' within the NCA: tackling organised crime, border policing, economic crime and the work of the Child Exploitation and Online Protection Centre (CEOP).[170,171] Much like SOCA, the NCA will gather intelligence to build the picture of serious organised crime, and its officers will have police, immigration or customs powers as necessary. The NCA will continue to operate SOCA's extensive overseas network and take forward the latter's focus on disrupting organised crime groups in addition to arrests and prosecutions.

190. The one significant difference between SOCA and the new NCA is the creation of a national tasking and co-ordination function. If the new NCA has only the same level of surveillance and enforcement resources to devote to operational activity as SOCA does, it will be reliant on local police forces to pursue joint investigations. This currently takes place on the basis of local and mainly informal agreements: SOCA cannot force other bodies to contribute towards countering national threats. The new tasking power is therefore crucial and a key development over the existing system. We asked the Home Secretary what powers would be available to ensure that local Police and Crime Commissioners would be required to support the NCA. She told us:

> *… we are looking at the moment in relation to the local police forces as to what the legislation should say and [whether] there should be… a statutory right for the NCA in relation to tasking… For this to work well, of course, the ideal is that you don't need to have powers to require police forces at a local level to get involved in operations where the NCA has identified a priority, but for that to be a natural part of the operation that takes place between police forces and the NCA.*[172]

---

[170] *CEOP will retain its operational independence and branding under the NCA.*

[171] *The NCA will also house its own dedicated national centre of expertise on cyber crime.*

[172] *Oral Evidence – Home Secretary, 19 January 2012.*

RESOURCES

Funding

Single Intelligence Account

191. The Single Intelligence Account (SIA) represents the total funding for the three intelligence and security Agencies. The 2010 Spending Review (SR10) provided a flat-cash settlement of approximately £2bn for the SIA over the four-year period beginning April 2011.[173]

	2011/12	2012/13	2013/14	2014/15
Single Intelligence Account (£m)[174]	1,928	1,961	1,979	1,954
Cyber security funding and Critical Capability Pool funding (£m)[175]	70	154	90	105

192. In our last Annual Report, we expressed concern that the impact of inflation may erode the Agencies' capabilities, since a flat-cash settlement could represent a real-terms cut of up to 11%.[176] This is something we discussed with all three Agency Heads and with the National Security Adviser, in his capacity as Principal Accounting Officer for the SIA.

193. We were told that the pressure on budgets had been manageable, in part due to public sector pay constraints, but also because the Agencies had put pressure on suppliers to reduce their costs. The National Security Adviser told the Committee that "*my first six-month assessment is that these reductions have not handicapped the Agencies' ability to respond to high priorities*".[177]

T. In our 2010–2011 Annual Report, we expressed concern about the impact of a flat-cash settlement on the Agencies' capabilities over the Spending Review period. It would appear that public sector pay constraints and the Agencies' efforts to control other costs have allowed capabilities to be maintained. This is reassuring in the short term, but we remain of the opinion that the Spending Review settlement must be kept under review to ensure that it is commensurate with the threat.

Agency expenditure

194. The charts below show the Agencies' capital and resource expenditure (in 'near-cash' terms) for 2010/11 to 2012/13.[178]

---

[173] *The SIA also includes funding for the National Cyber Security Programme, elements of the Critical Capability Pool funding and funding for a small part of the National Security Secretariat in the Cabinet Office. Since SR10 there have been changes to the SIA settlement to take account of transfers between departments and the public sector pay restraint announced in the Chancellor's Autumn Budget Statement.*

[174] *SIA settlement – 'near-cash' (Resource DEL plus Capital DEL, excluding depreciation and Annually Managed Expenditure), excluding ring-fenced funding for cyber security.*

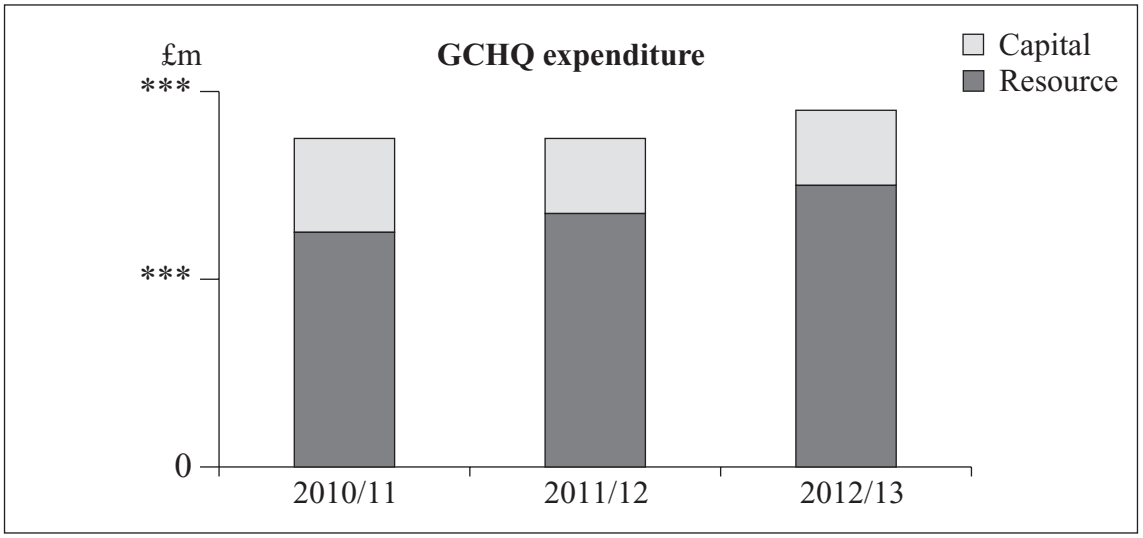
[175] *Resource DEL plus Capital DEL.*

[176] *Cm 8114.*

[177] *Oral Evidence – National Security Adviser, 20 October 2011.*

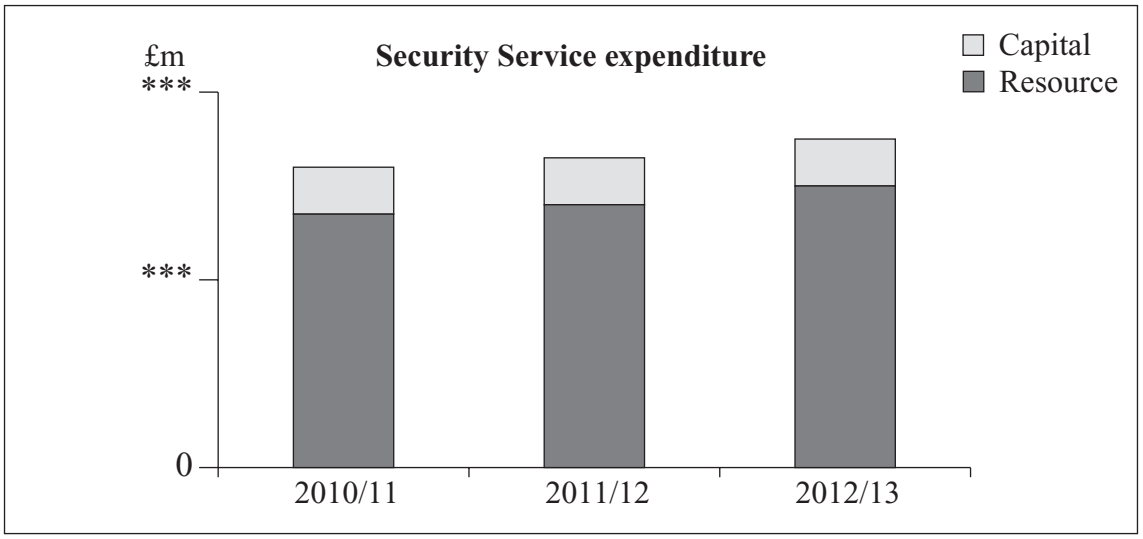
[178] *'Near-cash' (Resource DEL plus Capital DEL, excluding depreciation, amortisation and Annually Managed Expenditure), excluding ring-fenced funding for cyber security. Figures for 2010/11 are actual outturn and those for 2011/12 are provisional outturn. Figures for 2012/13 are based on budgets from the Main Estimate.*

195. GCHQ's total spend in 2010/11 was £***m (of which 24% was capital). Total expenditure for 2011/12 increased by 2.7%.[179]



GCHQ's 2010/11 accounts were certified by the Comptroller and Auditor General on 7 July 2011 with an unqualified audit opinion. The National Audit Office's (NAO's) audit found no significant problems.

196. The Security Service's total expenditure for 2010/11 was £***m (of which capital spend represented approximately 17%). Expenditure for 2011/12 increased by approximately 1%.[180]



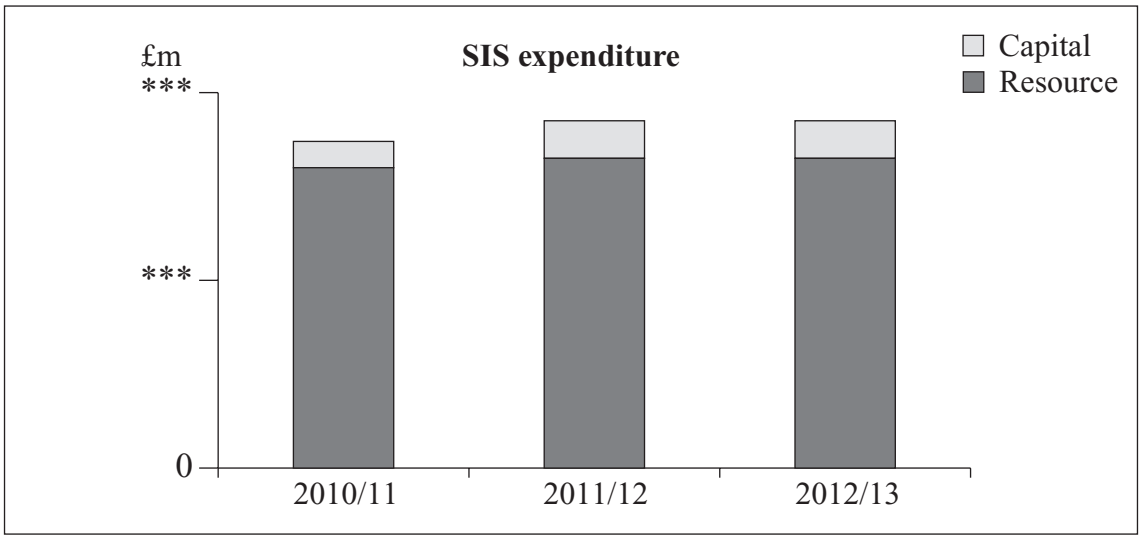
The Security Service's Annual Accounts were certified by the Comptroller and Auditor General on 7 July 2011 with an unqualified audit opinion. The NAO's audit of the accounts identified a number of significant issues which required corrective action by the Service. These issues concerned weaknesses relating to financial management; obtaining of Principal Accounting Officer approval for expenditure above delegated authority limits;

[179] *2010/11 and 2011/12 expenditure calculated on a 'near-cash' basis (Resource DEL plus Capital DEL, excluding depreciation, amortisation and Annually Managed Expenditure), excluding ring-fenced funding for cyber security. 2011/12 figures are provisional.*

[180] *Ibid.*

the recording of losses; accounting for agent expenditure and early severance liabilities; and obtaining HM Treasury dispensation for specific spending. While a number of these findings demonstrated weaknesses in financial management procedures, the NAO noted that the Service had responded positively to resolving these issues, and that action was being taken to prevent any recurrence.

197. SIS's total spend for 2010/11 was £***m (of which capital spend was 8.5%). Total expenditure increased by 4.8% in 2011/12. [181]



The SIS Resource Accounts were certified by the Comptroller and Auditor General on 7 July 2011 with an unqualified audit opinion. The NAO's audits[182] found a number of significant issues, including: controlling operational expenditure; exceeding HM Treasury spending limits; and the completeness of the Fixed Asset Register. The NAO reports that SIS is taking steps to tighten its financial controls to prevent such problems in the future.

Capital projects

198. In recent years, all three Agencies have embarked on major IT and estates projects. These are aimed at improving the use of technology (both in terms of their investigative and operational work, and also their headquarters IT systems and networks), refurbishing accommodation, increasing resilience and business continuity, and improving collaborative working across the intelligence community.

199. GCHQ, as a technology-focused organisation, runs the largest capital programme across the SIA. Known as the Corporate Technical Investment Portfolio (CTIP), it absorbs a considerable proportion of the SIA (over £***m per annum) and is designed to modernise and enhance GCHQ's IT infrastructure and Signals Intelligence (SIGINT) collection and processing capabilities. The CTIP programme consists of a number of major projects, including:

- Mastering the Internet: delivering new capabilities including those relating to cyber security, network defence and improvements relating to ***;
- Support to Military Operations: ***;

[181] *Ibid.*
[182] *Refers to both interim and final.*

- Transforming Analysis: including improving collaborative working (both within GCHQ and with external agencies) to provide more effective and timely analysis and reporting of intelligence;
- IT Services: the provision of network infrastructure, IT systems and improvement to cyber security capabilities;
- National Technical Assistance Centre: provision of specialist technical services and support to law enforcement and intelligence and security Agencies as part of GCHQ's interception of communications mission;
- Better Business: including the provision and enhancement of corporate programmes such as electronic data and records management, HR and finance systems; and
- Facilities Management.

200. Given the size and complexity of CTIP, we commissioned our Investigator to scrutinise its structure and overarching governance. His report concluded that, overall, GCHQ manages its investments in a professional and competent manner. Nonetheless, the Committee was concerned about one project (to replace and upgrade the Agency's desktop IT systems) which was encountering difficulties. We therefore commissioned the NAO to carry out a value-for-money study. At the time of writing the NAO has completed its investigation and the Committee is considering its findings.

201. In last year's Annual Report, the Committee described GCHQ's estates strategy as "*haphazard*" and said GCHQ must "*develop a sensible long-term strategy for its accommodation requirements*".[183] GCHQ's estates strategy has been reviewed and is now more focused on the long term and is co-ordinated with the other Agencies. This is a welcome improvement. GCHQ told us:

> *We took on board the feedback of the ISC, as a result of your Report last year. I'm about to take it to the GCHQ board in the next month or two and update the estates strategy for the department. We are doing that in conjunction with the wider SIA estate strategy, to make sure the two are consistent. Very much the focus up to today is about rationalising the wider SIA estate, because of the financial pressures on Government generally and on the SIA itself. So the closure of Oakley and the opening of [a new site in Cheltenham] were very much in line with those principles.*[184]

202. The additional capacity at the new site in Cheltenham is now available, with the transfer of personnel from GCHQ's Oakley site having been completed by the end of 2011. The NAO reported to the Committee that the project was delivered on schedule and the costs are expected to be less than originally envisaged. It is estimated that this single change to its accommodation arrangements will save over £9m a year from the end of 2011/12.

203. The Security Service is undertaking a number of major projects covering estates, business continuity, core IT systems and improving its digital investigative capabilities. A notable success during the reporting period was the completion of the Digital Intelligence (DIGINT) programme, which aimed to improve systems for the collection and analysis of intelligence material gathered electronically. The Director General explained:

---

[183] *Cm 8114.*

[184] *Oral Evidence – GCHQ, 1 March 2012.*

> *One of the things that really drove us on the investment of DIGINT was a discussion where the relevant directors explained that actually, of all the material that we've caught, over half was not being processed. Now, as an intelligence organisation, that's a nightmare. I mean, quite frankly, I would rather not have the intelligence at all and miss something than have the intelligence and not actually having processed it… We have made real progress on that, and I'm very proud on DIGINT.*[185]

204. The DIGINT project was completed in April 2011 and has dramatically improved the efficiency and management of the Service's digital intelligence, resulting in the capability to process significantly greater volumes of digital intelligence material.

205. A number of other Security Service capital projects are suffering delays – although not, at this stage, any significant cost overruns – due to technical issues or commercial problems. We reported last year that the Service's new electronic records management system was in some difficulties and that the decision had been taken to postpone implementation of the new system until after the Olympics. However, this year we were told that the supplier would be unable to meet this new timetable, and the contract therefore had been terminated.

206. While the delay of this project will impact on the Service's ability to conduct complete searches of its records, the Service maintains that it has made further progress this year around rationalisation of legacy material and improvements to its ability to search for and recover data. The project is still in a transition phase, but the Service remains confident that, once completed, it will be "*substantially better placed to access and exploit our information comprehensively*".[186]

207. The Chief of SIS summarised the aims of his Service's capital programmes, which are heavily focused on IT, data and communications systems:

> *What we're trying to do through our investment programme is to improve the Service's resilience, the handling of our data, the storage of our data and the migration of our data, including our business continuity back-up arrangement. We're trying to build a technology for the future of the Service, so that we have a modular architecture whereby we can build the facilities and programmes for our purposes for the future in a much more interoperable way.*[187]

208. At £***m, the IT programme is the Service's most expensive capital investment programme. It consists of four individual projects and is due to be completed by March 2013. The main features and benefits of the programme include: internet capabilities; secure communications; improvements to software applications; updating information and communications systems; and SIS's contribution to a Joint Data Centre with the Security Service.

209. SIS is also planning to undertake a major programme of refurbishment to its UK estate. The programme will cost £***m over the next two years and comprises two strands. The first strand is a key enabler for the Service's other IT projects and requires the rewiring of SIS's headquarters in London to replace network cabling which is becoming obsolete. The second strand of the project is to refurbish offices to introduce open-plan

[185] *Oral Evidence – Security Service, 23 February 2012.*
[186] *Written Evidence – Security Service, 30 September 2011.*
[187] *Oral Evidence – SIS, 2 February 2012.*

working. This will increase capacity, allowing other parts of the estate to be rationalised, but is also expected to improve working methods and enhance collaborative working.

Efficiencies and savings

210. All three Agencies are facing significant pressure to deliver efficiencies and savings as part of the SR10 settlement. The table below shows the scale of the efficiencies required expressed as a percentage of each Agency's 2010/11 total budget:

Efficiencies (%)	**2011/12**	**2012/13**	**2013/14**	**2014/15**
GCHQ efficiency targets	5.1	8.3	12.0	12.0
Security Service efficiency targets	5.9	6.2	6.2	6.4
SIS efficiency targets	4.7	6.1	7.4	7.9

211. The efficiencies to be delivered during the SR10 period are extremely challenging. While detailed plans to achieve these savings are still being finalised, it would seem that there are some common areas which are likely to be targeted. These include the cancellation of previous plans to increase staff numbers, pressure on suppliers to control or reduce costs, and the increased use of SIA-wide commercial agreements.

212. In addition to the efficiencies required in each individual Agency, there are also SIA-wide efficiencies to be achieved over the SR10 period through joint working and shared corporate services (such as joint human resources, procurement, and finance functions). These additional savings will be crucial if the Agencies are to maintain capabilities in the face of frozen budgets. They are shown in the table below:

Collaborative working savings (£m)	**2011/12**	**2012/13**	**2013/14**	**2014/15**
Collaborative working efficiencies	0.0	40.0	85.0	95.0

213. There are clear benefits to be realised by merging corporate functions. However, we are concerned about the scale of savings. Many of the plans to make collaborative savings appear to derive from the same areas of work (e.g. procurement, IT services) as those that the Agencies are targeting to achieve internal savings. It would seem unlikely that the scale of savings envisaged can be delivered twice (i.e. through internal efficiency measures and through collaborative working). Indeed, the Chief of SIS said as much to the Committee in January 2011:

> *The area where I'm more reserved is whether there are many additional savings to be had on the corporate side through merging our HR and finance arrangements, for example. All three Agencies have had their SR10 settlements based on cutting the administration costs of the Agencies by… one-third. We can do that internally or we can do it through collaboration, but we can't do it twice. We can't save 33.3% internally and then save another chunk by collaborating with one another. That is a bridge too far.*[188]

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

214. In addition, the Committee was concerned to be told this year that, of the £220m in collaborative savings that has been demanded from the Agencies over the SR10 period, as at the beginning of 2011/12 plans were in place to realise only £158m, leaving a gap of £62m.[189] Even the plans for £158m of savings appear vague and unsubstantiated: the largest element of this – described as savings in 'wider investment', and amounting to £72m – is, we have been told, "*the least mature element of the collaborative savings agenda*".[190] In fact it appeared that none of the plans had much detail behind them and we have subsequently been told that "*substantial resources*" have been committed "*to develop plans for the key elements*". Although further detailed planning is now under way, the tri-Agency Board overseeing the delivery of the £220m savings admits that:

> *Although targets have been identified for all work streams… [there is] still further work required to develop delivery plans for all elements.*[191]

U. The Spending Review settlement for the Single Intelligence Account (SIA) was predicated on the Agencies finding substantial efficiencies in order to maintain capabilities. We are not yet convinced that these efficiencies are achievable, particularly in the case of collaborative working. We recommend that the central team under the National Security Adviser, who are in charge of the SIA, urgently re-evaluate the evidence base for, and viability of, these savings.

Staffing

Staff numbers

215. As with funding, the significant growth in staff numbers[192] which all three Agencies have experienced over the last decade is levelling off:

- GCHQ had 5,393 staff in March 2009, increasing to 5,675 by March 2010. However, this increase has now reversed, with numbers falling to 5,306 by March 2011.
- The Security Service had 3,656 staff in March 2009, increasing to 3,780 by March 2010. In March 2011, the workforce stood at 3,617.[193]
- SIS had 2,437 staff in March 2009, increasing to 2,682 by March 2010. In March 2011, SIS had 2,686 staff.

216. While overall numbers may be stabilising, staff turnover was high in the Security Service and SIS:

- In GCHQ, 451 staff left and 163.5 staff joined during 2010/11.
- In the Security Service, 342 staff left and 306 staff joined.[194]
- In SIS, 118 staff left and 132 staff joined.

---

[189] *Written Evidence – Security Service, 30 September 2011.*
[190] *Written Evidence – Security Service, 12 April 2012.*
[191] *Ibid.*
[192] *All staffing figures are Full Time Equivalent (FTE) unless otherwise stated.*
[193] *We note that the Security Service was due to increase staffing levels in 2011/12 as part of planning for the Olympics, and as a result of the extra money from the Government to develop the Service's work on cyber security and also to maintain its Counter-Terrorism capability following the move from Control Orders to Terrorism Prevention and Investigation Measures.*
[194] *The Security Service has said that these figures were unusually high for 2010/11, due to their redundancy programmes.*

Redundancies

217. In March 2011, Government spending cuts designed to reduce the budget deficit were predicted to result in over 400,000 job losses in the public sector over the period 2010/11 to 2015/16.[195] This figure has since been revised upwards, with the latest estimate being 730,000 by 2016/17.[196] The Agencies have not been immune to these pressures, and each has run its own voluntary severance or redundancy programme.

218. In GCHQ, 255 staff left on Approved Early Retirement terms in 2010/11. The cost of these exit packages to GCHQ was £23m. The Director of GCHQ told us that he had been forced to offer early retirement in order to reduce his staff numbers and stay within budget:

> *We lost a number of more senior members of staff as well and I would say that... as they walked out the door, as I shook hands with each of them, I felt a degree of regret, but we needed to get our figures down in order to hit our own Spending Review commitments and it also gave us an opportunity to refresh our workforce and so on.*[197]

219. In the Security Service, 216 staff left under the Service's Living Within our Means (LWOM) scheme in 2010/11. Of these, 103 staff left on voluntary terms and the remaining 113 on redundancy terms, as provided for by the Civil Service Compensation Scheme. The cost of the exit packages to the Security Service was £20m.[198] The Director General explained that one of the drivers for running the Service's redundancy campaign was to "*[change] the staff mix*", and that "*in this sort of world where technologies come and go in a fortnight, some of the staff that we had... weren't really the right people for that world*". He added that approximately 70% of the staff who had left under the LWOM scheme had "*limited postability, which is to say [it's] quite hard to find anything useful for them to do*".[199]

220. In SIS, 24 staff left under the terms of the Civil Service Compensation Scheme in 2010/11, at a cost to the Service of £3.95m.[200] The Chief explained that SIS had sought to lose a percentage of people at the top – i.e. those who cost the most. This explains why the departures cost SIS so much more than the other two Agencies, which managed to keep costs down. (The average cost of each SIS departure was about £166,000 compared with £93,000 and £90,000 for the Security Service and GCHQ respectively.)

V. The redundancy processes all three Agencies have now undertaken have cost the taxpayer significant sums. However, all three have reassured us that this was necessary in order to meet Spending Review savings targets. Moreover, they have cited further benefits in terms of less top-heavy and leaner organisations, and staff with more up-to-date specialist skills. We expect to see the impact of this restructuring emerge over the coming years.

---

[195] *Cm 8036.*
[196] *Cm 8303.*
[197] *Oral Evidence – GCHQ, 1 March 2012.*
[198] *NAO briefing – Security Service, January 2012.*
[199] *Oral Evidence – Security Service, 23 February 2011.*
[200] *NAO briefing – SIS, January 2012.*

Diversity

221. At senior levels, all three Agencies are largely white, male-dominated organisations. They have begun to take steps towards increasing the diversity of their staff, although progress is lacklustre. Improvements can be seen in female to male ratios, but the Agencies have had less success in diversifying their ethnic composition.[201]

SCS equivalent grades	Male	Female
GCHQ	79%	21%
Security Service	79%	21%
SIS	88%	12%

222. At 31 March 2011, of the 47 Senior Civil Servant (SCS) equivalents in GCHQ, only ten were female (21%). This compares with 35% across the workforce.[202] The Director of GCHQ told us:

> *… it's moving in the right direction, but [I'm] absolutely not sanguine with it and I will say, before anybody else says, I think it is not good enough.*[203]

GCHQ is working to increase the representation of women in the workforce by targeted advertising of jobs and initiatives such as sponsorship of the Institution of Engineering and Technology Young Woman Engineer of the Year award.[204]

223. Of the 47 SCS equivalents in the Security Service, ten are female (21.3%).[205] This compares with 40% across the organisation at all grades. The Director General said he was actively trying to encourage the promotion of more women, but that they had had only limited success:

> *Given that we are a Service where two of the Director Generals have been women… we have found it rather more difficult than one might have expected to attract female applicants, and I don't know why that is, although it must be something to do with the perception of what the Service does… We have been deliberately targeting our recruitment to attract female applicants and we have slightly improved, although it's still less than 50%.*[206]

224. Of the 99 SCS equivalents in SIS, only 12% are female.[207] This figure is particularly significant given the high proportion of SCS in the organisation (3.7% compared with 1.3% and 0.8% in Security Service and GCHQ respectively). The Chief explained that the percentage of women employed reflected the percentage of women who applied. However, SIS had recently launched a new recruitment campaign designed to attract more women. Efforts were being made to address retention rates for women in mid-career, with training and coaching being provided to encourage them to take on managerial roles and job-sharing being promoted in some operational roles. SIS acknowledged that it needed

---

[201] *All figures in the table represent headcount as at March 2011.*
[202] *Written Evidence – GCHQ, 18 November 2011.*
[203] *Oral Evidence – GCHQ, 1 March 2012.*
[204] *Ibid.*
[205] *Written Evidence – Security Service, 30 September 2011.*
[206] *Oral Evidence – Security Service, 23 February 2012.*
[207] *Written Evidence – SIS, 3 October 2012.*

to do better on diversity, both in terms of gender and ethnicity, where it faced significant problems:

> *We do have a serious diversity problem in SIS, and it's not just gender but gender is one of the biggest and most visible examples of the diversity problem. I think we've done better on skills diversity than we have on what you might call visible diversity, gender and ethnic diversity.*[208]

225. The statistics on ethnicity are similarly poor across all three organisations:[209]

SCS equivalent grades	White	Undeclared
GCHQ	87%	13%
Security Service	94%	6%
SIS	62%	38%

226. In GCHQ, 87% of the 47 SCS equivalents declared themselves as white; the remainder chose not to declare their ethnicity.[210] As a result of previous criticism, including by this Committee, GCHQ has taken action, introducing mandatory diversity training, sponsoring the Windsor Fellowship (a programme to attract black and minority ethnic applicants)[211] and introducing a programme to determine if there was any unintended bias in its selection processes.

227. In the Security Service, 94% of the 47 SCS equivalents declared themselves as white, with the remaining staff not declaring their ethnic background. While there has been some progress recruiting more minority ethnic staff over the years, senior managers remain predominantly white; efforts to increase diversity will take some time to work through the system. The Director General said that he recognised the value to the Service of a more diverse workforce:

> *We are deliberately targeting our advertising at black and minority ethnic [BME] staff, candidates and also female BME candidates, not least because, for operational reasons, we need people like that, because… if you look like me, then you can't operate in the operational areas that we need to operate in. So we are making progress on that, but it takes time for that to filter through the sort of hierarchy of the Service.*[212]

228. In SIS, 62% of the 99 SCS equivalents declared themselves as white (again, the remainder chose not to declare their ethnicity).[213] The Chief promised to improve the diversity of the organisation: "*We will work for a diverse leadership at director level, both diverse in terms of skills and experience and in terms of gender.*"[214]

229. Whilst diversity figures are slow to change, we note that the Security Service in particular has made a real effort to create an inclusive working environment. This has been

---

[208] *Oral Evidence – SIS, 2 February 2012.*
[209] *All figures in the table represent headcount as at 31 March 2011.*
[210] *GCHQ Annual Report and Accounts 2010–2011.*
[211] *Oral Evidence – GCHQ, 1 March 2012.*
[212] *Oral Evidence – Security Service, 23 February 2012.*
[213] *Written Evidence – SIS, 3 October 2011.*
[214] *Oral Evidence – SIS, 2 February 2012.*

recognised by their high score on the Stonewall Index – a workplace equality index which ranks employers' performance in areas such as tackling anti-gay bullying and harassment, and supporting the career development of lesbian, gay and bisexual employees.

W. All three Agencies apply the same nationality requirements, which are a pre-requisite for security clearance. Whilst that does hamper their recruitment of a more ethnically diverse workforce, we nevertheless consider that greater efforts can, and must, be made even within these constraints.

Staff retention

230. The Chief of SIS told us that staff retention was becoming a problem for all the Agencies "*and that is a reflection on the increasing problem we face about the pay and conditions that we can offer staff*".[215] This was impacting on morale and on the discretionary effort that people were willing to put in. He said:

> *people are less likely to go the extra mile and do the more dangerous thing or take that added level of risk if they feel that they are not being recognised for it and that their rewards are somehow inadequate… Now, this is a growing problem… It's not just me. Jonathan Evans and Iain Lobban have similar challenges… the sense that our staff are not being properly recognised for the challenges and responsibilities that they face is becoming an increasing issue.*[216]

He went on to suggest that this problem needed to be addressed:

> *We need to find a way, not just within existing resource and existing systems to improve the recognition and the reward to people, but we may have to do something which recognises that the staff of the intelligence agencies, a bit like the police or the armed forces, do something that's unique and those unique qualities should be recognised.*[217]

231. However, the real concern for this Committee is the ability of GCHQ to retain internet specialists to respond to the threat to UK cyber security. In our 2010–2011 Annual Report we recommended that GCHQ explore ways to improve the situation and that the Cabinet Office, as lead department for cyber security, should consider employing a system of bonuses for specialist skills, such as is used in the US. This year we were told that the situation had deteriorated and that GCHQ was "*losing critical staff with high end cyber technology skills at up to three times the rate of the corporate average (3.4%)*".[218]

232. The Director thought this problem was likely to increase in the coming years. He explained that there was a growing market for cyber security experts and government could not match the salaries that industry was offering. As a result GCHQ was training staff who were then recruited by the private sector, attracted by higher salaries and greater benefits. He strongly suggested that a new employment model, which created mutual benefits for government and industry from trained cyber experts, was needed:

---

[215] *Ibid.*
[216] *Ibid.*
[217] *Ibid.*
[218] *Written Evidence – GCHQ, 20 April 2012.*

… this picture is not going to change and so one of the things that I'm looking at is whether or not we can recruit people, train them and then employ them with the expectation… of losing them at the end of that period… and, as they move into industry, for them to be useful for us. If they're working with some of those companies that we work very closely with, perhaps there is a benefit that we can get from them.[219]

X. GCHQ's continuing difficulties retaining internet specialists is a matter of grave concern. We have asked the Director of GCHQ to identify options to address the problem of how to retain such specialist staff, which can then be discussed with the Cabinet Office and HM Treasury. We expect to see a package agreed and implemented before the start of the 2013/14 financial year.

Consultants and contractors

233. In our 2010–2011 Annual Report, we noted the increasing reliance of the Agencies on consultants and contractors, in particular to deliver their technology programmes. We criticised the rapid growth of expenditure in this area, and commissioned our Investigator to report on the background to, expansion of and justifications for such spending.

Key findings from the Investigator's report on consultants and contractors

- In common with many government departments, the Agencies had arrived at their current high level of contractor and consultant use through a combination of design and historical drift.
- There is a question as to whether the Agencies are 'trapped' in the contractors' net, particularly in the field of IT.
- The Agencies have developed robust business cases and project monitoring processes, but they lacked a comprehensive way of assessing whether or not their use of contractors and consultants actually offered value for money.
- There were several signs of recent improvement: progress had been made on standardising terminology; joint procurement, especially on shared IT services, had commenced; and the Agencies were determined to move away from costly 'time and materials' contracts to product- or benefit-based ones.
- The Cabinet Office had a greater role to play in co-ordinating and examining the efforts of the three Agencies in this area, and there were signs that its 'hands off' approach was slowly changing.

234. The Committee was reassured by the Investigator's conclusion that there was, for the most part, sufficient retained expertise within the Agencies to act as an 'intelligent customer' in setting requirements and monitoring delivery by contractors. However, it is clear that, primarily due to vetting considerations, there remains a limited pool of security-cleared contractors from which the Agencies can choose for high-end IT contracts. This could impact on value for money for the public. In addition, closer working between the

[219] *Oral Evidence – GCHQ, 1 March 2012.*

Agencies and a more strategic approach to what business is outsourced over the medium term would give greater reassurance that the Agencies were obtaining value for money.

235. The National Security Adviser, on behalf of the Agencies, accepted in full all but one of the recommendations in the Investigator's report.[220] He emphasised that the Agencies are "*committed to driving increasing value*" from their expenditure on contractors and consultants, and pledged to "*continue to develop a wider range of suppliers*" to ensure value for money.[221]

236. We subsequently questioned each of the Agencies on how they planned to implement the report's recommendations. SIS told us that it was developing "*a clear plan about the skills that we intend to outsource and the ones we need to keep over the next decade*",[222] and that it had merged its procurement department with that of the Security Service, which has already saved £22m through more aggressive negotiations with its suppliers. The Director General of the Security Service commented that:

> *I think it would be a fair criticism to say that we have had some cases where [our use of consultants and contractors] hasn't been as controlled as it should, [but now] we have got a proper focus… post-Olympics, we intend to reduce [the] number of organisations and individuals we deal with and to manage those relationships more aggressively than we have done.*[223]

237. GCHQ noted that:

> *… part of our workforce still have some way to go in terms of recognising our true partnership with industry and how critical that is to delivery… within GCHQ there is some inherent bias against using industry… I don't believe we should have a bias for or against industry, the bias should be making sure the delivery is value for money.*[224]

Y. The Agencies spend hundreds of millions of pounds of public money every year with industry. They have a responsibility to ensure that in doing so they achieve value for money. The Committee is pleased that the Government has responded positively to our Investigator's recommendations in this area, and will look to see what improvements are made over the remainder of the Spending Review period.

---

[220] *One of the recommendations was only partially accepted: the National Security Adviser did not accept that the Agencies should bring contracted work back inside the organisation. However, the Committee considers that, where it is appropriate, such work should be brought inside and the Agencies should plan to do so; we are therefore discussing this further with the National Security Adviser.*

[221] *Letter from the National Security Adviser, 8 December 2011.*

[222] *Oral Evidence – SIS, 2 February 2012.*

[223] *Oral Evidence – Security Service, 23 February 2012.*

[224] *Oral Evidence – GCHQ, 1 March 2012.*

OTHER ISSUES

Gareth Williams

238. The Committee reported last year on the death of Gareth Williams. The body of Mr Williams, who was on secondment to SIS from GCHQ, was discovered in his central London flat in August 2010. Following a police investigation, an inquest into the circumstances of his death was held at Westminster Coroner's Court in April 2012.

239. There has been extensive media coverage of Mr Williams' death, much of it containing allegations around his personal life, both following the discovery of his body and, more recently, during the Coroner's proceedings. These have clearly been deeply distressing for the Williams family. This speculation has also made understanding any implications of Mr Williams' death for the Agencies more difficult. Last year the Director of GCHQ told us he found the media coverage "*deeply frustrating and irritating… I am frustrated by the fact that getting a single truth about activities he may or may not have been involved in… is quite difficult*".[225]

The Coroner's inquest and verdict

240. The inquest began on 23 April 2012 and reported on 2 May. The Coroner recorded a narrative verdict, which said:

> *The cause of his death was unnatural and likely to have been criminally mediated. I am therefore satisfied on the balance of probabilities that Gareth was killed unlawfully.*[226]

241. The Coroner's public statement indicated that there was no evidence that Mr Williams' death was linked to his work with the Agencies. Nevertheless, she was critical about management failures which resulted in a considerable delay in the escalation of Mr Williams' unexplained absence from work to the police. The Chief of SIS has publicly and unreservedly apologised for this failure.[227]

Concerns arising from the case about SIS and GCHQ procedures

242. The police continue their enquiries into Mr Williams' death, and the case remains open. Nevertheless, the case raises some general issues about procedures at both SIS and GCHQ, and the Committee has questioned both Agencies on these aspects.

Duty of care

243. It took SIS a week to take any action when Mr Williams failed to turn up for work. This seems extraordinary, given that Agency staff are inevitably at risk due to the nature of the work that they are involved in. The Coroner was critical of these management failures – which were largely those of SIS.

244. After the inquest SIS explained that it had reviewed its absence reporting procedures after Mr Williams' death. It told us it had "*taken steps to ensure that all line managers*

---

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

[226] *Her Majesty's Coroner, Inquisition – Gareth Wyn Williams.*

[227] *See e.g. 'Gareth Williams "probably" killed unlawfully', BBC News, 2 May 2012.*

are aware of their responsibilities and that we have clear processes in place to allow concerns to be escalated quickly to locate missing members of staff".[228]

245. We asked for more detail on these arrangements and were told that SIS's review of absence reporting had concluded that "*whilst the policies themselves were correct, they had not been communicated strongly enough and so understanding and implementation were weaker than they should have been*."[229] All staff had since been made aware of policies on recording their own leave and reporting colleagues' unexpected absences.[230] We have had sight of SIS's revised 'taking care' practice sheet which is distributed to all its employees, and which sets out in detail the steps to be taken by staff if they notice that one of their colleagues is absent.[231] SIS told us that "*line managers have a key responsibility to take action immediately, and escalate if necessary, when it is noticed someone is not where they should or might be, or is unaccountably absent*".[232]

246. As Mr Williams' employing Agency, GCHQ told us it had also changed its procedures for notification and management of staff absences to ensure that there are clear lines of responsibility for reporting absences and that all staff are aware of their responsibilities. It had reviewed thoroughly and updated its arrangements for staff on secondment to the other Agencies:

> *The responsibilities of staff members whether notifying or being notified of absence are clearly laid out, pointing up in particular what needs to happen in respect of staff in 'singleton' posts and where staff are absent and have not made contact.*[233]

Co-operation with the police

247. There have been reports in the media that SIS did not co-operate fully with the police and had withheld evidence from the investigation team. SIS has rejected these reports as being "*without foundation*"[234] and told us that it has at all times co-operated fully with SO15 in connection with this investigation, a point which the senior SO15 officer giving evidence made during the inquest. SIS further told us that new procedures have been put in place, with SIS having direct contact with the investigation team in the Metropolitan Police, without any intermediate step.

The vetting process

248. The Committee has considered the issues raised by Mr Williams' death with regard to the adequacy of the vetting regime. There have been a number of allegations about Mr Williams' private life. The Coroner took evidence on these matters and addressed them in her summing up. It is also important to note that an individual's lifestyle choices are not an automatic bar to holding a security clearance. However, there is a general issue around what GCHQ and SIS know about their employees' personal lives: the more detail that the Agencies know about their employees, the easier any risk is to manage.

249. Responsibility for Mr Williams' vetting lay with GCHQ. His first Developed Vetting (DV) clearance was granted in 1999 when he was in the final stages of completing a PhD

[228] *Letter from SIS – 3 May 2012.*
[229] *Letter from SIS – 17 May 2012.*
[230] *Ibid.*
[231] *Letter from SIS – 31 May 2012.*
[232] *Ibid.*
[233] *Letter from GCHQ – 21 May 2012.*
[234] *Letter from SIS – 31 May 2012.*

at the University of Manchester. He then underwent a routine review in 2001 after his first year in GCHQ,[235] which assessed him as representing a 'very low' risk. Mr Williams underwent a further full vetting review after five years in GCHQ – which is standard practice – which confirmed the 'very low' risk rating. His next review was due in 2011. GCHQ has told us that its practice "*exceeds national standards while balancing the need to maintain a reasonable and proportionate level of intrusion*".[236]

250. SIS told us it had called for and reviewed Mr Williams' vetting file before his secondment commenced and had no reason to question the 'very low' risk assessment by GCHQ.[237]

Z. The Inquiry into the death of Gareth Williams has taken nearly two years, during which there has been much media speculation as to the reasons behind Mr Williams' death. We extend our sympathy to the family of Mr Williams who have had to endure continuous intrusion under very difficult circumstances. There is no doubt that determining the cause of death was made more complex by the unnecessary delays in reporting Mr Williams' unexplained absence from work. SIS has rightly apologised for this. SIS and GCHQ, Mr Williams' home department, have reviewed their arrangements, including for staff on secondment. We consider that the Agencies must exercise a far greater duty of care in relation to their employees than other organisations, owing to the nature of the work they are involved in.

[235] *This review after the first year is an additional step carried out by GCHQ.*
[236] *Letter from GCHQ – 21 May 2012.*
[237] *Letter from SIS – 17 May 2012.*

LIST OF RECOMMENDATIONS AND CONCLUSIONS

A. It is imperative that policy implications and analytical judgements remain separate in any intelligence assessment provided to Ministers. We are reassured that Ministers recognise the importance of this distinction and that it will be maintained.

B. The Committee recognises that it is often impossible to predict how and when events such as the 'Arab Spring' will begin, and it is understandable that the intelligence community was taken by surprise, as indeed were the governments in the countries affected. There is a question, however, as to whether the Agencies should have been able to anticipate how events might subsequently unfold, and whether the fact that they did not realise that the unrest would spread so rapidly across the Arab world demonstrates a lack of understanding about the region. Events over the past 18 months have shown the need for the intelligence and security Agencies to maintain a global coverage, in addition to the strategic priorities set by the National Security Council and the Joint Intelligence Committee.

C. We commend the Agencies for their rapid reaction to the 'Arab Spring' once events became clear, and their very significant contribution to the UK's response. They demonstrated agility and flexibility in reprioritising their resources and providing the National Security Council with the intelligence it needed to form the UK response.

D. The Committee considers that the failure in one notable case this year demonstrates a lack of operational planning that we would not have expected from SIS and other participants. The imperative to take action quickly dominated at the expense of thorough and effective planning. It was an ill-considered approach that misjudged the nature and level of risk involved. We recognise, however, that SIS did implement a thorough review, following this failure, and appears to have taken the lessons seriously. We would have expected nothing less.

E. The Agencies have continued to see notable successes in their Counter-Terrorism work. It is clear that this is becoming more challenging and, despite increases in resources, they still face difficult decisions when prioritising their efforts against the most pressing threats. Given that the Agencies' recent growth will not continue over the coming years, the challenge will be to get the most out of current resources through more innovative – and where appropriate collaborative – working. The Committee welcomes the progress the Agencies are making in this regard.

F. We recognise that the Security Service has taken all possible measures to make available the necessary resources during the period of the Olympic and Paralympic Games, but remain concerned at the risk that is being taken in some areas and the vulnerability of the UK at this critical period.

G. The Olympic and Paralympic Games have placed all three Agencies (particularly the Security Service) under unprecedented pressure this year. The Committee recognises the exceptional effort that has been required from the staff of all three during this time.

H. The Committee is concerned about the potential increase in overall risk as a result of the introduction of the Terrorism Prevention and Investigation Measures (TPIMs) regime. The lack of any direct correlation between risk levels and the additional funding

made available to the Security Service and police to prepare for this only adds to our unease, as do the delays in putting the funding in place prior to the transition from Control Orders.

I. Given the increased risk associated with the TPIMs regime, we welcome the Government's move to make additional powers available should the circumstances demand. However, the 'Enhanced' TPIMs proposals do not appear to be practical or workable, and it seems unlikely that they would ever be implemented.

J. Prevent is a key strand of the Government's Counter-Terrorism Strategy and the Committee will continue to monitor this important work. The Research, Information and Communications Unit's counter-radicalisation work is progressing, albeit slowly. We understand that counter-ideological work may take some time. However, the Committee continues to be concerned about the lack of measures to assess the effectiveness of the strategy. Whilst we recognise the difficulties involved, it is nevertheless important that ways are found to identify and assess the results of this work and the resources being used.

K. The provision of Information Assurance advice to government, businesses and the public has the potential to generate the greatest improvement in UK cyber security for the least cost. The Communications-Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI), among others, continue to provide an invaluable service to businesses and government departments in this regard. Nonetheless, educating users and individuals about basic information security has significant potential and should be a greater focus for the National Cyber Security Programme.

L. We recommended last year that the Deputy National Security Adviser should prioritise the development of an effective funding model for the Communications-Electronics Security Group (CESG). To a certain extent the problem has been addressed through short-term funding arrangements. However, the importance of CESG's Information Assurance work requires that a long-term funding model must be established.

M. Twenty months into the National Cyber Security Programme, there appears to have been some progress on developing cyber capabilities. However, cyber security is a fast-paced field and delays in developing our capabilities give our enemies the advantage. We are therefore concerned that much of the work to protect UK interests in cyberspace is still at an early stage.

N. The transition to internet-based communication, and the emergence of social networking and instant messaging, have transformed the way people communicate. The current legislative framework – which already allows the police and intelligence and security Agencies to access this material under tightly defined circumstances – does not cover these new forms of communication.

O. The prospect of Iran acquiring nuclear weapons is of serious concern. The UK must continue, with our international partners, to apply diplomatic and economic pressure to persuade the Iranian regime to alter its course. We support the Government's efforts, and those of the Agencies, whose work against this threat is invaluable.

P. The UK does not condone, solicit or encourage torture or cruel, inhuman or degrading treatment (CIDT). However, to protect the UK our Agencies must work with foreign agencies, some of whom do not meet our standards. In so doing, there is a risk that our Agencies will, indirectly and inadvertently, be linked to such activities. It is unfortunate, but inescapable, that those risks cannot always be wholly eliminated. The challenge therefore is how to minimise that risk, while maintaining essential intelligence-sharing relationships with our international partners.

Q. The Committee understands the reasons for halting the current Detainee Inquiry and supports the Government's plans to hold another judge-led Inquiry when possible. The specific allegations of UK involvement in renditions of two individuals to Libya remain under police investigation and we will, therefore, not be commenting further at this time.

R. Defence Intelligence makes a critical contribution to the UK's intelligence collection and assessment capabilities. However, it is often not thought of as part of the central intelligence machinery and the Committee is concerned that its vital role sometimes goes unrecognised. We hope that the reforms will result in DI obtaining the profile its work deserves.

S. Defence Intelligence has told us that it "*can't cover everything all the time in the modern world*". Nevertheless, Strategic Defence and Security Review cuts will further decrease DI's ability to provide global coverage with sufficient depth. It is therefore likely that even greater risk will have to be taken when reacting to the next crisis than was the case with the Libya campaign. This is an unsatisfactory position. We urge the Government to ensure that sufficient resources are available to allow in-depth coverage to be maintained on an ongoing basis.

T. In our 2010–2011 Annual Report, we expressed concern about the impact of a flat-cash settlement on the Agencies' capabilities over the Spending Review period. It would appear that public sector pay constraints and the Agencies' efforts to control other costs have allowed capabilities to be maintained. This is reassuring in the short term, but we remain of the opinion that the Spending Review settlement must be kept under review to ensure that it is commensurate with the threat.

U. The Spending Review settlement for the Single Intelligence Account (SIA) was predicated on the Agencies finding substantial efficiencies in order to maintain capabilities. We are not yet convinced that these efficiencies are achievable, particularly in the case of collaborative working. We recommend that the central team under the National Security Adviser, who are in charge of the SIA, urgently re-evaluate the evidence base for, and viability of, these savings.

V. The redundancy processes all three Agencies have now undertaken have cost the taxpayer significant sums. However, all three have reassured us that this was necessary in order to meet Spending Review savings targets. Moreover, they have cited further benefits in terms of less top-heavy and leaner organisations, and staff with more up-to-date specialist skills. We expect to see the impact of this restructuring emerge over the coming years.

W. All three Agencies apply the same nationality requirements, which are a pre-requisite for security clearance. Whilst that does hamper their recruitment of a more ethnically diverse workforce, we nevertheless consider that greater efforts can, and must, be made even within these constraints.

X. GCHQ's continuing difficulties retaining internet specialists is a matter of grave concern. We have asked the Director of GCHQ to identify options to address the problem of how to retain such specialist staff, which can then be discussed with the Cabinet Office and HM Treasury. We expect to see a package agreed and implemented before the start of the 2013/14 financial year.

Y. The Agencies spend hundreds of millions of pounds of public money every year with industry. They have a responsibility to ensure that in doing so they achieve value for money. The Committee is pleased that the Government has responded positively to our Investigator's recommendations in this area, and will look to see what improvements are made over the remainder of the Spending Review period.

Z. The Inquiry into the death of Gareth Williams has taken nearly two years, during which there has been much media speculation as to the reasons behind Mr Williams' death. We extend our sympathy to the family of Mr Williams who have had to endure continuous intrusion under very difficult circumstances. There is no doubt that determining the cause of death was made more complex by the unnecessary delays in reporting Mr Williams' unexplained absence from work. SIS has rightly apologised for this. SIS and GCHQ, Mr Williams' home department, have reviewed their arrangements, including for staff on secondment. We consider that the Agencies must exercise a far greater duty of care in relation to their employees than other organisations, owing to the nature of the work they are involved in.

GLOSSARY

AQ	Al-Qaeda
AQAP	Al-Qaeda in the Arabian Peninsula
BME	Black and Minority Ethnic
CCD	Communications Capabilities Development
CDI	Chief of Defence Intelligence
CESG	Communications-Electronics Security Group
CIDT	Cruel, inhuman or degrading treatment
CMPs	Closed material procedures
CONTEST	UK Counter-Terrorism Strategy
CPNI	Centre for the Protection of National Infrastructure
CSP	Communication Service Provider
CTIP	Corporate Technical Investment Portfolio
DCMS	Department for Culture, Media and Sport
DI	Defence Intelligence
DIGINT	Digital Intelligence
ECHR	European Convention on Human Rights
FATA	Federally Administered Tribal Areas (Pakistan)
GCHQ	Government Communications Headquarters
HUMINT	Human Intelligence
IAEA	International Atomic Energy Authority
ICT	International Counter-Terrorism
IED	Improvised Explosive Device
ISC	Intelligence and Security Committee
IT	Information Technology

JIC	Joint Intelligence Committee
JTAC	Joint Terrorism Analysis Centre
MoD	Ministry of Defence
NAO	National Audit Office
NCA	National Crime Agency
NCSP	National Cyber Security Programme
NSC	National Security Council
NSS	National Security Strategy
OSCT	Office for Security and Counter-Terrorism
PII	Public Interest Immunity
R&Ps	Requirements and Priorities
RICU	Research, Information and Communications Unit
RIPA	Regulation of Investigatory Powers Act 2000
RIRA	Real Irish Republican Army
SCS	Senior Civil Servant
SIA	Single Intelligence Account
SIGINT	Signals Intelligence
SIS	Secret Intelligence Service
SOCA	Serious Organised Crime Agency
SR10	Spending Review 2010
TPIMs	Terrorism Prevention and Investigation Measures

LIST OF WITNESSES

Ministers

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

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

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Mr Iain Lobban CB – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Sawers KCMG – Chief, SIS

Other officials

SECURITY SERVICE

Mr Jonathan Evans – Director General, Security Service

Other officials

DEFENCE INTELLIGENCE

Vice Admiral Alan Richards RN – Chief of Defence Intelligence

Other officials

CABINET OFFICE

Sir Peter Ricketts GCMG – National Security Adviser (until December 2011)

Sir Kim Darroch KCMG – National Security Adviser (from January 2012)

Paul Rimmer – Director, Central Intelligence Assessment

Other officials