Intelligence and Security Committee of Parliament

Annual Report 2012–2013

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

Intelligence and Security Committee of Parliament – Annual Report 2012–2013

TSO

TSO
information & publishing solutions

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

Online
www.tsoshop.co.uk

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

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

TSO@Blackwell and other accredited agents

ISBN 978-0-10-298652-5

9 780102 986525

Intelligence and Security Committee of Parliament

Annual Report 2012–2013

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

Presented to Parliament pursuant to section 3 of the Justice and Security Act 2013

Ordered by the House of Commons to be printed on 10 July 2013

HC 547 £16.00

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

ISBN: 9780102986525

Printed in the UK by The Stationery Office Limited

on behalf of the Controller of Her Majesty's Stationery Office

ID: 2573953 07/13

Printed on paper containing 75% recycled fibre content minimum.

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

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 CH 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 of Parliament (ISC) is a statutory committee of Parliament that has responsibility for oversight of the UK intelligence community. The Committee was originally established by the Intelligence Services Act 1994, and has recently been reformed by the Justice and Security Act 2013.

The Committee oversees the intelligence and security activities of the UK, including the policies, expenditure, administration and operations of the Security Service (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). The Committee also scrutinises the work of other parts of the UK intelligence community, including 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 Committee consists of nine Members drawn from both Houses of Parliament. The Chair is elected by its Members. The Members of the Committee are subject to Section 1(1)(b) of the Official Secrets Act 1989 and are routinely given access to highly classified material in carrying out their duties.

The Committee sets its own agenda and work programme. It takes evidence from Government Ministers, the Heads of the intelligence and security Agencies, officials from the intelligence community, and other witnesses as required. The Committee is supported in its work by an independent Secretariat and an Investigator. It also has access to legal and financial expertise where necessary.

The Committee produces an Annual Report on the discharge of its functions. The Committee may also produce Reports on specific investigations. Prior to the Committee publishing its Reports, sensitive material that would damage national security is 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. The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted, rather than keeping this secret. This means that the Report that is published is the same as the classified version sent to the Prime Minister (albeit with redactions): there is no 'secret' report.

CONTENTS

SECTION 1: THE WORK OF THE COMMITTEE 3

SECTION 2: KEY FINDINGS ON THE PERFORMANCE OF THE AGENCIES 4

SECTION 3: THE AGENCIES' ASSESSMENT OF THE THREAT 6

SECTION 4: COUNTER-TERRORISM 9
- The Security Service response 12
- Operational collaboration 13
- Overseas partners 14
- Northern Ireland-related terrorism 15
- Terrorism Prevention and Investigation Measures (TPIMs) 16

SECTION 5: CYBER SECURITY 18
- Cyber defence: government and industry 18
- 'Disruption' and military cyber 19
- Resourcing cyber security 20

SECTION 6: COUNTER-PROLIFERATION 23
- Intelligence on the Iranian nuclear programme 23
- Syria 24
- North Korea 25
- Pakistan 25
- Collaborative working: the 'virtual hub' 25

SECTION 7: SUPPORT TO MILITARY OPERATIONS 27
- Afghanistan 27
- Resourcing 29

SECTION 8: WIDER INTELLIGENCE ISSUES 31
- Legislation 31
- The Joint Intelligence Committee 32

SECTION 9: AGENCY EXPENDITURE 34
- Major projects 35
- Efficiencies and savings 36
- Staffing 40

SECTION 10: REFORM OF THE INTELLIGENCE AND SECURITY COMMITTEE 42

ANNEX A: AGENCY STRATEGIC OBJECTIVES 44

ANNEX B: SCOPE 45

LIST OF RECOMMENDATIONS AND CONCLUSIONS 47

GLOSSARY 50

LIST OF WITNESSES 52

SECTION 1: THE WORK OF THE COMMITTEE

1. This Report details the work and conclusions of the Intelligence and Security Committee of Parliament (ISC) for the period covering July 2012 to June 2013. During this time, the Committee has:

- held 15 formal evidence sessions with, amongst others, the three intelligence Agencies,[1] Defence Intelligence, the Chair of the Joint Intelligence Committee, the National Security Adviser, and the Foreign and Home Secretaries;
- held ten further full Committee meetings and 34 other meetings;
- visited the Agencies and other parts of the intelligence community for informal briefings on seven occasions;
- held bilateral discussions with those in the American intelligence community; and
- hosted delegations from Australia, Cyprus, Denmark, Hungary, Israel and Pakistan.

2. The Committee has taken evidence on and examined the work of the three intelligence and security Agencies and the wider intelligence community, which is the subject of this Report. In addition we have reported to the Prime Minister on a number of highly sensitive matters, and published reports on two specific matters:

(i) In February 2013, we published a report on '*Access to communications data by the intelligence and security Agencies*'.[2] This focused on the proposals in the draft Communications Data Bill, on which we took evidence from the intelligence community, a number of UK-based Communications Service Providers and BAE Systems Detica. The final 28-page report contained 19 recommendations and conclusions; further detail can be found on page 31.

(ii) In June 2013, we reported on '*Foreign Involvement in the Critical National Infrastructure.*'[3] This focused on one particular case in the telecommunications industry, but looked at the processes and procedures that should be in place for assessing the risks associated with foreign investment in the UK's Critical National Infrastructure. The 23-page report contains nine recommendations and conclusions: at the time of writing we are awaiting the Government's response to them.

3. In addition to these matters, a further issue that we have focused on this year was the passage of the Justice and Security Act through Parliament, which gained Royal Assent in April. Part 1 of the Act aimed to strengthen the ISC and provide it with enhanced powers and resources, and Part 2 introduced Closed Material Procedures in civil courts. In terms of the ISC, it was necessary to ensure that the Committee's remit and powers reflected the considerable changes in the intelligence world since the Committee was first established in 1994. We welcome the changes in the Act, which are broadly in line with those we ourselves had previously recommended to the Government, and which will increase accountability. We consider the detail of the changes on page 42 and the other aspects of the Act on page 31.

---

[1] *The Security Service, the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ).*
[2] *Cm 8514.*
[3] *Cm 8629.*

SECTION 2: KEY FINDINGS ON THE PERFORMANCE OF THE AGENCIES

4. This was an exceptionally demanding year for the Agencies, not least due to the pressures of ensuring a safe and successful Olympic and Paralympic Games. The Games represented the largest intelligence and security challenge that the Agencies have ever faced in peacetime. We commend those working in the Agencies for their considerable efforts, and congratulate all those involved on the successful outcome.

5. Against this backdrop, we have considered how well the Agencies have responded to the main threats that the UK has faced over the last year. The Agencies receive nearly £2bn of public money each year. In the current economic climate, it is essential that this level of funding can be justified. One of the ways in which the Agencies' performance is measured is through the agreements they have with HM Treasury, which sets Agency Strategic Objectives (ASOs). In 2012/13, the Agencies worked on a total of 11 ASOs between them, covering their primary areas of effort (including counter-terrorism, cyber security, counter-proliferation, counter-espionage, supporting the UK's Armed Forces, and maintaining the ability to respond to unexpected events). The ASOs are listed at the end of this Report at Annex A.

6. There have been significant achievements by the Agencies over the past year against these ASOs. It is clear that the Agencies have expanded their coverage of terrorist activity, particularly outside the UK, where the number of groups that have to be investigated is increasing as Al-Qaeda becomes more fragmented. Recent convictions (detailed at paragraph 21) show that there are still individuals and groups who intend to carry out attacks in the UK. The Agencies are working more collaboratively on operations to gather intelligence across the range of their work. Through investment in technology, they have also increased their ability to monitor cyber threats, although they acknowledge that the overall scale of the threat is considerable, and this is an area where more resources are required. Ensuring that they can recruit and retain staff with the specialist skills required for this highly technical work remains an area of concern, despite progress on its reward packages (we cover this in more detail at paragraph 55).

7. Our assessment is that the Agencies continue to meet their operational tasks, demonstrating innovation, professionalism and commitment that we are keen to acknowledge. The Committee continues to be impressed with the dedication and tenacity of Agency staff, and we note the increasing importance of collaborative working, both between the Agencies and with partners overseas, in maintaining this level of success.

8. While the Agencies' efforts to keep the UK safe remain impressive, the Committee has a number of concerns. Most significant of these is with regard to the collaborative savings programme. Last year we noted our concerns that plans were not in place to achieve the full £220m of savings needed. We have not seen much improvement this year. Indeed, the Agencies' original Corporate Services Transformation Programme (CSTP) to transform the way in which they deliver corporate services such as HR, finance and vetting has been shut down (see paragraph 115). Such problems when working together on corporate issues are in stark contrast to the Agencies' strengths when collaborating on operations. We expect to see considerable improvements on the plans for the remaining years of the 2010 Spending Review (SR10) period if crucial front-line capabilities are to

be safeguarded: with less than two years of the Spending Review period left, this remains one of the Committee's key concerns.

9. Sir Jonathan Evans stepped down as Director General of the Security Service in April this year. Sir Jonathan led the Service successfully for over five years: we thank him for his outstanding contribution and for the very positive way in which he engaged with this Committee. We wish him well for the future.

SECTION 3: THE AGENCIES' ASSESSMENT OF THE THREAT

10. The threat to the United Kingdom and its interests overseas continues to come from a number of different sources, as outlined in previous Annual Reports, including international and Northern Ireland-related terrorism, Hostile Foreign Activity and nuclear proliferation. The intelligence and security Agencies, Defence Intelligence and the wider intelligence community work to counter these threats. The following is a summary of their current threat assessment.[4, 5]

THE CURRENT THREAT PICTURE

The threat to the UK from international terrorism

The UK threat level from international terrorism is SUBSTANTIAL, indicating that an attack is a strong possibility. Al-Qaeda Core has continued to operate despite significant pressure in the Federally Administered Tribal Areas (FATA) of Pakistan.

The threat from Al-Qaeda has diversified: although all Al-Qaeda affiliates retain significant intent, their capabilities and opportunities vary. The greatest risk of attack on UK soil is posed by Al-Qaeda-inspired but self-organised groups, particularly those who have sought advice and training from extremists in the FATA of Pakistan. UK citizens living or working in areas where extremists operate face a continuing risk of kidnap.

The Joint Terrorism Analysis Centre (JTAC) assesses that Al-Qaeda in the Arabian Peninsula has been pushed back into its safe havens in Yemen. However, the organisation retains the intent and capability to conduct attacks: it therefore represents an enduring threat to the UK. It is likely to take advantage of any opportunity to strike at Western interests in the region and an attack could materialise with little or no notice.

In Somalia, al-Shabaab has been weakened as a cohesive group. The Security Service assesses that it is, however, still capable of mounting attacks throughout the region, including against Western targets.

Al-Qaeda in the Maghreb (AQM) has been pushed back into remote strongholds by French and Malian military action but it has not been completely neutralised. The attack by an AQM splinter group against the gas facility at In Amenas, Algeria, in January 2013 demonstrated the nature of the threat posed by Islamists in the region to British interests, which is likely to be enduring. However, AQM and its affiliates do not yet pose a direct threat in the UK.

[4] *Assessments of the level and nature of the threat from international terrorism are made by the Joint Terrorism Analysis Centre (JTAC); the Security Service is responsible for setting the threat levels from Irish and other domestic terrorism both in Northern Ireland and Great Britain. There are five tiers to the threat level system: CRITICAL (an attack is expected imminently); SEVERE (an attack is highly likely); SUBSTANTIAL (an attack is a strong possibility); MODERATE (an attack is possible, but not likely); and LOW (an attack is unlikely).*

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

The Agencies and JTAC assess that Al-Qaeda elements and individual *jihadists* in Syria currently represent the most worrying emerging terrorist threat to the UK and the West. There is a risk of extremist elements in Syria taking advantage of the permissive environment to develop external attack plans, including against Western targets. Large numbers of radicalised individuals have been attracted to the country, including significant numbers from the UK and Europe. They are likely to acquire expertise and experience which could significantly increase the threat posed when they return home. Furthermore, there is growing concern about the risks around extremist groups in Syria gaining access to regime stocks of chemical weapons.

In North Africa, state weakness in the developing democracies of Tunisia, Libya and Egypt offers space for the development of extremist Islamist groups. In Libya, the attack on the US Consulate in Benghazi in September 2012 and small scale attacks against UK diplomatic interests demonstrate how this threat can manifest itself. Tunisia is seeing increasing activity by extreme Salafist groups with anti-Western sentiment. In Egypt the authorities arrested an extremist cell which may have been planning attacks in Egypt.

Northern Ireland-related terrorism

There continues to be a serious threat of terrorism in Northern Ireland, principally from dissident republican terrorist groups, and the threat level in Northern Ireland remains SEVERE (an attack is highly likely). The Northern Ireland-related terrorist threat to the rest of the UK was reduced in October 2012 to MODERATE (an attack is possible, but not likely).

Whilst the dissident republican groups lack a coherent political agenda and have little popular support, the threat remains serious. In 2012 there were 24 attacks (compared with 26 in 2011 and 40 in 2010). While the majority of these were unsophisticated, several displayed significant lethal intent. Dissident republicans will attack any security force target, depending on opportunity. The Police Service of Northern Ireland (PSNI) remains the main focus largely because of its visibility; last year, a number of police officers narrowly escaped injury.

In 2012, the emergence of a new dissident republican group (calling itself the IRA) following the merger of the Real Irish Republican Army (RIRA), a group of unaffiliated dissident republicans and a republican vigilante group reversed the trend towards fragmentation of dissident republican groups. This new group was responsible for the murder of prison officer David Black on 1 November 2012 and has attempted a number of attacks which have been disrupted by the security forces. There are indications that other dissident republican groups have become more active in response to the emergence of this new grouping.

The cyber threat

The UK faces a threat of hostile cyber activity from criminals, other states and, potentially, terrorists. There is major activity by criminals seeking to defraud individuals and businesses. However, the internet also provides new opportunities for states to conduct espionage against the UK. State-sponsored cyber espionage is happening on a large scale and targets intellectual property and sensitive commercial information across the UK economy, in addition to government classified information.

The UK also faces a threat of cyber attacks that result in the disruption of a computer network. There have been several such incidents against US financial institutions and foreign energy companies. Most of these have taken the form of 'denial of service' attacks (where a huge amount of data is sent to a network or system in order to prevent legitimate users from accessing a site or service). Separately, some have involved the deletion of large amounts of data from corporate computer systems.

Hostile Foreign Activity
The threat to British interests from espionage remains high, and the UK continues to be a high-priority target for a number of foreign intelligence services. These services actively seek to obtain official and commercially sensitive intelligence in their governments' national interests. The commercial sector as well as government, technology, defence and security interests are at risk from both 'traditional' espionage and hostile activity conducted in cyberspace.

Proliferation of Weapons of Mass Destruction (WMD)
The UK continues to support international efforts to prevent WMD proliferation in the Middle East and North Korea. Both are of significant concern. Iran continues to expand its nuclear programme and has hitherto failed to engage seriously in negotiations to address international concerns. The threat to regional stability remains extremely high if Iran develops or acquires viable nuclear weapons technology, or reneges on its non-proliferation treaty obligations.

SECTION 4: COUNTER-TERRORISM

11. Despite the increased profile of other threats to the UK (such as cyber security, which is covered later in this Report), counter-terrorism work remains the primary focus of the intelligence and security Agencies. Their work – analysing intelligence to understand better where threats might originate, and helping to prevent attacks before they happen – is distinct from that of the rest of Government, and is crucial. ***.

12. The evolution of the threat that we described in our 2011–2012 Annual Report[6] has continued: the Agencies have told us that the terrorist threat to the UK is now "*more diverse and multifaceted than it has been in recent years*".[7] Al-Qaeda and its affiliates[8] are expanding into a wider range of countries and are seeking to exploit ungoverned or unstable spaces, including across the Sahel and North Africa. The former Director General of the Security Service summarised the situation as follows:

> *I think 18 months ago or two years ago I would... probably have been slightly more positive about the overall trajectory [of the threat]. The reason that I have a bit of caution about that is because of the impact of the so-called Arab Spring, so that Al-Qaeda, who were very much boxed into certain areas, particularly Pakistan, and suffering as a result of the American drones programme, they now have the ability to operate in parts of the Arab world where they have not been before, and that makes the picture more complex.*[9]

A summary of the current assessment of Al-Qaeda and its affiliates is set out overleaf.

13. The Security Service has expressed concern about the growing collaboration between Al-Qaeda affiliate organisations at both strategic and operational levels. ***.

14. There is also an increasing potential for those who travel overseas to train and fight alongside one of the Al-Qaeda affiliate groups to subsequently return to the UK and pose a direct threat to the UK's national security. We mentioned last year that there was a small contingent of UK citizens based in Somalia fighting alongside Al-Shabaab. UK residents continue to travel to Pakistan to train with Al-Qaeda Core. Most significant, however, is the growing trend for UK-resident extremists to join Islamist elements of the opposition in Syria, which is likely to form part of the terrorist threat picture for years to come.

---

6 *Cm 8403.*

7 *Written Evidence – Security Service, 10 September 2012.*

8 *Al-Qaeda affiliates include Al-Qaeda in the Arabian Peninsula (AQAP), Al-Qaeda in the Maghreb (AQM), Al-Qaeda in Iraq (AQI), and Al Shabaab.*

9 *Oral Evidence – Security Service, 17 January 2013.*

AL-QAEDA AND ITS AFFILIATES

Al-Qaeda Core

- Al-Qaeda Core in the FATA of Pakistan has continued to weaken, but still poses the greatest strategic threat to the UK.
- It accounted for the most significant proportion of international counter-terrorism investigations in the first quarter of 2012/13.[10]
- Its capability to carry out a mass casualty attack has diminished, but there remains a risk of a repeat of an event such as the 2005 London bombings, either inspired or directed by Al-Qaeda Core.
- Relatively smaller scale attacks have emerged as an alternative modus operandi.

Al Shabaab in Somalia

- Al Shabaab in Somalia is believed to be linked to attacks in other countries in the region, and there remains a risk to UK interests.
- A mixture of AMISOM[11] military gains and leadership tensions has weakened the group.
- We have been told that the threat to the UK has reduced as extremists seek alternative countries in which to engage in *jihad*.
- There is a consistently high threat to Western interests from Al Shabaab: ***. Al Shabaab also has the capability to reach beyond Somalia's borders.
- Considerable risks remain. Divisions in the Al Shabaab leadership could increase the threat, leading to a dispersal of the threat to the wider region; giving Western foreign fighters more freedom to plan attacks or leave for other theatres of *jihad*.

Al-Qaeda in the Arabian Peninsula

- The former Director General assessed the threat from Al-Qaeda in the Arabian Peninsula (AQAP) in Yemen as still high.
- The Foreign Secretary described AQAP as "*probably the most innovative [franchise]"*[12] as seen from the unsuccessful aviation bomb plot in 2012.
- We have been told that AQAP retains the intent and the capability to attack the West.

[10] *In contrast, in previous years investigations linked to Pakistan have accounted for up to three-quarters of all plots.*
[11] *African Union Mission in Somalia.*
[12] *Oral Evidence – Foreign Secretary, 22 November 2012.*

Al-Qaeda in the Maghreb (AQM)

- Al-Qaeda in the Maghreb remains of concern given the lack of governance in the region.
- The Government has assessed that Al-Qaeda-related groups in North Africa are "*stronger… than ever before and have greater freedom of movement*".[13]
- We have been told that this region is a "*growth area for terrorism*",[14] and the Foreign Secretary told us that a direct threat to the UK could emerge from the area "*if we don't deal successfully with the problems in Mali and in Northern Nigeria in particular*".[15]
- These have carried out a number of attacks against Western interests, international organisations (such as the United Nations) and civilian targets. They maintain an ongoing intent to kidnap Western nationals in the region.

Al-Qaeda in Iraq (AQI) and the Al-Nusrah Front (ANF)

- AQI continues to focus on the Government of Iraq and sectarian targets in Iraq, and does not pose a direct threat to the UK at present.
- ANF is an 'offshoot' of AQI based in Syria that *** has access to significant numbers of foreign fighters, including UK nationals.

15. In addition to those returning to the UK, 'lone actors' (those who have no substantive links to terrorist groups) also continue to pose a significant threat. We heard from the Home Office this year that:

> *There is no doubt that the more sophisticated people in Al-Qaeda recognise that groups are, in some ways, a thing of the past; and that encouraging lone acts of terror is exactly the way forward.*[16]

16. There have been a small number of attacks in the UK carried out by lone actors – the stabbing of Stephen Timms, MP at a constituency surgery in 2010 being perhaps the most high profile. We have been told that the Security Service looks for signs of lone actors when assessing new intelligence, and refers vulnerable individuals to programmes designed to prevent them from being drawn into violent extremism.[17] However, we note that such risks are inherently much more difficult to manage: by their nature lone actors are much harder to detect.

17. The Security Service has told us that lone actor attacks inspired by extreme right-wing ideology (as opposed to Islamist extremism) are likely to be "*small scale… and lacking sophistication*".[18] However, in light of the attacks by Anders Breivik in Norway in 2011 which killed 77 people, we question whether this continues to be an accurate assessment.

---

[13] *Cm 8583.*
[14] *Written Evidence – Security Service, 10 September 2012.*
[15] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[16] *Oral Evidence – Home Office, 13 December 2012.*
[17] *Written Evidence – Security Service, 8 March 2013.*
[18] *Written Evidence – Security Service, 8 March 2013.*

A. Despite the increased profile of other threats such as cyber security, counter-terrorism work rightly remains the primary focus of the intelligence and security Agencies. Their work in analysing intelligence to understand the threat and seeking to help to prevent attacks remains crucial to our national security.

B. The shape of the terrorist threat is potentially changing from tightly organised cells under the control of structured hierarchies to looser networks of small groups and individuals who operate more independently. It is essential that the Agencies continue to make a clear assessment of this evolving picture in order to keep ahead of the threat and to help to prevent attacks and loss of life.

The Security Service response

18. The Security Service allocated 68% of its overall resources to International Counter-Terrorism (ICT) during 2011/12 (broadly similar to the previous two years). Actual spend on ICT increased by 2.6%. The Service *** cautions that its "*domestic assurance will never be complete*".[19]

19. In January 2013, we were told that the number of ICT investigations was "*at an all-time high*". We questioned the former Director General on the overall level of assurance that he was able to give. He told us:

> *I don't think the overall level of risk that we are running in the country has gone up in the last few years. Equally, I don't actually think that the intent and capability [of the terrorists] has gone down. The element that to some extent has changed gradually over the last five to seven years is the ability of the security authorities to identify and respond. We think that's been positive.*[20]

20. The Security Service continues to work closely with the police, and has a network of regional stations ***. In September 2012, the Security Service told the Committee that "*the regional counter-terrorist network and our close cooperation with the police are critical to our ability to counter terrorist threats, with the relationship between the police and the Security Service continuing to deepen and broaden*".[21]

SECURITY SERVICE CASE STUDY: REGIONAL NETWORK

When assessing the work of the Agencies this year, we looked at a number of sensitive case studies in detail. We cannot publish the detail of these studies due to national security concerns; however, this particular operation demonstrated the importance of the Security Service's regional network.

***.

21. This close collaboration has led to several high-profile successes for the Security Service:

- Four men from Luton were arrested in April 2012, and were convicted in April 2013 of planning terrorist acts.

---

[19] *Written Evidence – Security Service, 10 September 2012.*
[20] *Oral Evidence – Security Service, 17 January 2013.*
[21] *Written Evidence – Security Service, 10 September 2012.*

- In July 2012, several individuals were arrested and charged after they were found in possession of weapons and explosives in South Yorkshire. They were convicted in April 2013 after pleading guilty.
- Three men from London were arrested in July 2012, and convicted in April 2013 of a series of terrorist offences (this investigation involved the use of high-tech retrieval methods to collect information from their computer).
- ***.
- In February 2013, 11 men were convicted in connection with plotting attacks in the UK which they hoped would surpass the 7 July 2005 London bombings. Collectively, they received sentences amounting to 120 years in prison.

Whilst we commend the Security Service for these results, the numbers indicate the very significant threat the UK faces, and the importance of the Security Service's work.

22. The barbaric killing of Drummer Lee Rigby in Woolwich on 22 May this year was a tragic loss of life of a soldier who had done so much for our country. A criminal investigation into the attack is under way, and the police and the Security Service are working to establish the full facts of the case. The Prime Minister has asked this Committee to review the actions of the intelligence and security Agencies, and the counter-terrorism aspects of the police actions. We have agreed to investigate: at the time of writing we have received an initial submission of evidence from the Security Service and GCHQ. We expect to receive further submissions over the summer and will question witnesses in the autumn. We will publish our findings as soon and as fully as we are able (subject only to restrictions on grounds of national security or *sub judice* rules).

Operational collaboration

23. The trend that we noted last year for an increasing amount of counter-terrorism work to feature an 'upstream' element has continued ('upstream' refers to aspects of an investigation such as attack planning, preparation or direction occurring outside the UK, and terrorist groups with little or no presence in the UK). In the first three months of 2012/13, a significant proportion of the Security Service's ICT investigations "*were focussed on upstream threats which did not have a substantial UK footprint*".[22] This has driven closer working with SIS and GCHQ, who are able to collect intelligence and pursue disruptions overseas in support of these investigations.

24. In a report on collaborative working, our Investigator noted that in operational matters there has been:

> *… a huge change for the better, sweeping away the tired old turf wars of ten or twenty years ago. Each Agency has found that the skills of the others are critical to the success of their own operational mission…*[23]

The Committee attaches high importance to this joint approach on operational work, which demonstrates the Agencies' recognition of the skills each can bring to counter-terrorism work.

---

[22] *Written Evidence – Security Service, 10 September 2012.*

[23] *ISC Investigator: 'Scoping Paper On Collaborative Working In The Agencies', 4 December 2012.*

25. SIS and GCHQ devoted around a third of their efforts in 2011/12 to ICT work. These figures are expected to fall slightly in 2012/13, as the increased resources diverted to ICT in the run-up to and during the Olympics are reallocated to other areas. Nevertheless ICT will remain the greatest focus for both Agencies.

26. We have been given several examples of operational successes this year: SIS told us that it had expanded its coverage of certain countries and targets, and disrupted terrorist attack-planning.[24] Meanwhile GCHQ has discovered the location of a bomb-making factory, detected attack-planning and improved its understanding of terrorist networks.[25]

CASE STUDY: COLLABORATIVE APPROACH

The detail of this case study cannot be published for national security reasons. However, it highlighted the importance of close cooperation between the three intelligence Agencies in relation to 'upstream' counter-terrorism work.

***.[26, 27]

Overseas partners

27. Counter-terrorism work continues to necessitate close working not just with those in the UK intelligence community but also with overseas partners. SIS has a network of relationships with its overseas counterparts, and the Chief described to us the benefits that this could bring:

> *… countries will play to their strengths and the joy of partnership, as we all know, is that two people or two organisations bring different strengths to a partnership and the total is more than the sum of its parts and that is what we are trying to create…*[28]

Nevertheless, certain relationships are closer than others, and SIS has acknowledged that it needs to build up its contacts in new areas quickly, and remain agile as the terrorist threat shifts.

28. Whilst working in partnership brings benefits – and, indeed, is essential when working against the terrorist threat – it also brings real challenges. All three Agencies have noted that their work to disrupt plots is affected by a lack of identifiable partners, concerns over other governments' approaches to human rights or legal obligations, and/or those governments' low political will to tackle terrorist groups. We have been told that such barriers "*represent significant challenges to the aspiration… of building international cooperation against terrorism.*"[29] SIS explained that this sometimes constrained intelligence-sharing and limited joint working opportunities:

> *… when we try to… work at pace, we have to be very, very careful that we understand the parameters and how [other] countries are operating and what their legal basis is and what their framework is, particularly if we have intelligence which could*

---

[24] *Written Evidence – SIS, 11 September 2012.*
[25] *Written Evidence – GCHQ, 11 September 2012.*
[26] *Letter from the Security Service and SIS, 11 May 2012.*
[27] *Oral Evidence – Security Service, 17 January 2013.*
[28] *Oral Evidence – SIS, 24 January 2013.*
[29] *Written Evidence – Security Service, 10 September 2012.*

lead to a detention… It is hard and there will be some cases where, frankly, we will not get the assurances and we will not therefore be able to share intelligence which could lead to a detention in which we would have no control over how that individual is being treated.[30]

29. Whilst the UK Agencies may have a clear legal and ethical framework in place, the same cannot always be said for those that they must deal with. SIS has been running a number of projects to improve the capabilities and governance of security and legal institutions in countries such as *** to ensure that assurances on detainee treatment, for example, are sufficiently robust to allow SIS to share intelligence.

30. In 2010, this Committee considered the draft policy guidance on working with overseas partners, and made recommendations to the then Prime Minister as to the issues that needed to be addressed in this complex and difficult area. The overarching policy was subsequently published, and the Intelligence Services Commissioner now monitors the Agencies' compliance with it. The Commissioner reported:

I am not aware of any failure by a military or intelligence officer to comply with the Consolidated Guidance in the period between 1st January and December 31st 2011. I have received assurances from the relevant departments and intelligence agencies that they have disclosed fully relevant information about cases... I am also assured that I have been given full access to both information and officers to discuss particular cases both in the UK and during Station visits. I therefore have no reason to doubt that the guidance is being complied with... I can report that from what I have seen, the intelligence agencies and MOD take their human rights and legal obligations towards detainees seriously.[31]

Northern Ireland-related terrorism

31. The threat in Northern Ireland from dissident republican groups remains high, and we have seen numerous attacks or attempted attacks on the police and other security personnel. This included, in November 2012, the shooting of prison officer David Black as he drove to work. This was the first murder of a prison officer in Northern Ireland since 1993.

32. Although the number of national security attacks has remained broadly the same, a wider range of devices (some of which have been more sophisticated) have been deployed over the past year. The Home Secretary told us that "*there are some worrying signs*"[32] about the threat posed by these groups. The former Director General of the Security Service commented that:

… in my judgment [the threat] is not, overall, going up. But equally, nor is it being extinguished… there are still a significant number of people who are actively members of dissident republican terrorist groups… and some of those are very effective terrorists. They [still] want to attack. They know how to attack. They have the means to attack, and from time to time they will succeed in doing so.[33]

***.

---

[30] *Oral Evidence – SIS, 24 January 2013.*
[31] *Intelligence Services Commissioner, 2011 Annual Report, HC 497, 13 July 2012.*
[32] *Oral Evidence – Home Secretary, 14 December 2012.*
[33] *Oral Evidence – Security Service, 17 January 2013.*

33. The Security Service has, in recent years, increased the resources it devotes to countering the dissident republican threat. We have been told that, alongside the efforts of the Police Service of Northern Ireland (PSNI), this has improved the intelligence coverage of the threat, ***.[34] This has led to an increased number of arrests (around 200 in each of the last three years), which we have been told has had an effect in reducing the terrorists' capabilities. We understand that the greater coverage is leading to more disruption opportunities, which are an additional way (alongside arrests and seizures of weapons) of preventing attacks.

34. We have also been told that cooperation with the Irish Republic is extremely good and that this collaboration has also led to disruptions and arrests. The former Director General told us that:

> *Our co-operation on the whole with the Gardaí is very good… They have just as much political wish not to see a resurgence of Republican terrorism as we do… whilst they have continued to prioritise national security work, they don't have the resources that one might ideally have… but they are very co-operative and helpful to us, and quite often the disruptions and the arrests are collaborative between north and south.*[35]

35. The two main loyalist groups (the Ulster Defence Association and the Ulster Volunteer Force) remain committed to the political process. However, sectarian tensions remain heightened after the widespread disorder which followed the decision in December 2012 of Belfast City Council to limit the number of days on which the Union flag is flown at Belfast City Hall. Although these protests have subsided, they are continuing, and the Chief Constable of the PSNI has said publicly that individual members of the loyalist paramilitary groups were involved in orchestrating the disorder. The leadership of the groups did not seem to be organising the involvement of their members, and the loyalist ceasefires are assessed to be holding.

Terrorism Prevention and Investigation Measures (TPIMs)

36. We reported last year on the replacement of the Control Order regime with that of Terrorism Prevention and Investigation Measures (TPIMs). These came into force in January 2012. Since then, one individual subject to a TPIM has absconded – and at the time of writing is still at large – and another is alleged to have breached the conditions of his TPIM by travelling through an area from which he was excluded (the Olympic Park) on no fewer than five occasions. In the latter case, the Crown Prosecution Service declined to prosecute the individual for breaching the conditions of his TPIM. The Home Secretary commented:

> *I feel frustrated whenever I see a breach of a TPIM not being prosecuted. I also feel frustrated when I see the breach of a TPIM being prosecuted and the courts dismissing it, because they say it is just, sort of, normal natural behaviour or something. So there is a genuine issue which we have not yet found a solution to, about the point at which the CPS… and the courts will be willing to say: yes, this is a breach…*[36]

---

[34] *Written Evidence – Security Service, 10 September 2012.*
[35] *Oral Evidence – Security Service, 17 January 2013.*
[36] *Oral Evidence – Home Secretary, 14 December 2012.*

37. The Security Service (along with the police) has been allocated additional funding to increase its overall counter-terrorism capabilities, although this is not ring-fenced in relation to those individuals who have been placed on a TPIM. We have been told that this general increase in funding has resulted in an "*uplift in Security Service capability, which will help ensure that there is no substantial increase in overall ICT risk as a result of the move to the new regime*".[37]

38. In contrast to Control Orders, TPIMs have a two-year time limit, beyond which they cannot be extended. In evidence to the Joint Committee on Human Rights (JCHR), the Independent Reviewer of Terrorism Legislation, David Anderson QC, confirmed that he was in favour of the two-year limit, although he warned:

> *… its consequence is going to be that some people whom both the Home Secretary and the judges believe to be dangerous terrorists may be free of all constraint, in some cases at the beginning of next year. That is why I also say that it is tempting in some cases to wish for longer.*[38]

39. Nonetheless, Mr Anderson emphasised that the two-year limit would "*focus energies on finding an exit strategy*".[39] In his report examining the operation of TPIMs in 2012,[40] Mr Anderson suggested that more needs to be done in this area. He recommended that exit strategies should in future include the integration of any related PREVENT activity into the management of the TPIM, as well as giving consideration to some form of dialogue with subjects similar to that employed in the criminal courts, where the probation service proposes how an individual might best be rehabilitated. The Government published their response[41] to his report in May 2013, agreeing with this recommendation.

C. The Committee shares the concerns of the Independent Reviewer of Terrorism Legislation over what happens when individual Terrorism Prevention and Investigation Measures (TPIMs) come to the end of their two-year limit. The Government must take steps now to ensure that they have sufficient policies in place when TPIMs have reached their limit and cannot be extended.

---

[37] *Written Evidence – Security Service, 10 September 2012.*

[38] *Uncorrected transcript of oral evidence to the JCHR on Review of the TPIMs Regime, 19 March 2013.*

[39] *Ibid.*

[40] *First Report of the Independent Reviewer on the Operation of the TPIMs Act 2011, published March 2013.*

[41] *The Government Response to the Report by David Anderson QC on Terrorism Prevention and Investigation Measures in 2012, published in May 2013.*

SECTION 5: CYBER SECURITY

40. The Committee has been told this year that the threat from cyber attacks "*is at its highest level ever and is expected to rise further still*", with the identification of "*new actors and more evidence of serious hostile cyber activity*".[42]

41. The main focus of the intelligence and security Agencies' work on cyber is on countering Hostile Foreign Activity, covert intelligence gathering, ***.[43] The importance of the link between cyber and state threats can be seen from the recent decision by the Security Service to merge its work on counter-espionage, counter-intelligence, counter-proliferation, cyber and protective security into a new branch. The Security Service told us:

> *Foreign states… currently pose the principal cyber threat to national security. It makes sense therefore to brigade our cyber investigations with our other counter-espionage and counter intelligence investigations and assessment.*[44]

42. Whilst state actors continue to pose the greatest threat (China and Russia, for example, are alleged to be involved in cyber attacks), we have been told that a number of countries are also using private groups to carry out state-sponsored attacks. ***.[45] These state-affiliated groups consist of skilled cyber professionals, undertaking attacks on diverse targets such as financial institutions and energy companies. These groups pose a threat in their own right, but it is the combination of their capability and the objectives of their state backers which makes them of particular concern.

43. We note that there does not, as yet, appear to be a credible threat in cyberspace from terrorist groups such as Al-Qaeda. ***.[46] Nevertheless, terrorist groups may well pose a greater threat in cyberspace in future and this provides an additional impetus to ensure that the UK's cyber capabilities are of the highest standards in what is a fast-moving field.

Cyber defence: government and industry

44. Given the potential for the loss of sensitive information, protecting the Government's own IT systems is of crucial importance. In recent years, many government departments have come under cyber attack: often, this has involved websites being disrupted by 'denial of service' attacks,[47] and last summer over 200 email accounts across 30 government departments were targeted in an attempt to steal confidential information. It appears that the Government systems' defences are reasonably well developed, although evidence we have taken suggests that it is a constant challenge to ensure that cyber 'hygiene' is maintained (e.g. updating anti-virus software), and to ensure that cyber defences develop quickly in response to the changing nature of the attacks.[48]

---

[42] *Written Evidence – GCHQ, 11 September 2012.*

[43] *The majority of cyber attacks continue to be criminal, and therefore fall primarily to the police and law enforcement. However, the intelligence and security Agencies have worked with law enforcement to build their capacity and skills to investigate such crimes, and also with international partners to conduct investigations into those behind these attacks.*

[44] *Letter from the Security Service, 4 December 2012.*

[45] *Oral Evidence – GCHQ, 31 January 2013.*

[46] *Oral Evidence – GCHQ, 31 January 2013.*

[47] *A 'denial of service' attack aims to disrupt the website, making it unavailable to legitimate users, rather than to steal sensitive information.*

[48] *Oral Evidence – Defence Intelligence, 7 February 2013.*

45. Government departments are also targeted via attacks on industry suppliers which may hold government information on their own systems. We have been told that cyber espionage "*[has] resulted in MOD data being stolen*,***."[49] This has both security and financial consequences for the UK.

46. Hostile foreign actors also target UK businesses more generally. We have heard how the Government has worked, through the Communications-Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI), to raise the awareness of cyber security at board level in major companies. The Foreign Secretary told us that he had attempted "*to shock some companies in particular into taking more action… we put the argument to them: you wouldn't leave the doors of your offices open all night, so why do you do that with regard to cyber security?*"[50] The former Director General of the Security Service told us that as part of this work the Security Service had identified companies that had suffered financial losses as a result of cyber attacks. This gives the company an incentive to improve its defences:

> *One of them… concluded that they had lost at least £800 million as a result of *** cyber attacks, and that's quite a lot of money, even for a major company. But it's very helpful, because otherwise you are just saying, 'Well, some information has gone. So what?'*[51]

47. Another development we have been told about this year is the increased targeting of professional services firms (e.g. lawyers and accountants) as opposed to other, more obvious, targets who may have stronger defences. The Foreign Secretary told us that such a trend was "*worrying*", adding:

> *[These] are a route into a defence company, a high tech manufacturer, whoever it may be, who may have good defences themselves, but of course a lot of their data is sitting with their lawyers or their accountants and if they are soft targets, well, then it becomes quite easy to get that data a different way.*[52]

GCHQ added that there was a further facet to this activity, involving "*targeting through overseas subsidiaries… then swimming up the network on to the UK network*".[53]

D. The threat the UK is facing from cyber attacks is disturbing in its scale and complexity. The theft of intellectual property, personal details and classified information causes significant harm, both financial and non-financial. It is incumbent on everyone – individuals, companies and the Government – to take responsibility for their own cyber security. We support the Government's efforts to raise awareness and, more importantly, our nation's defences.

'Disruption' and military cyber

48. The Committee believes that another key aspect of work on cyber is what we refer to as 'disruption' or military cyber – this could involve disrupting an adversary's systems to prevent cyber attacks on the UK, or actions in cyberspace that support a conventional

---

[49] *Written Evidence – Defence Intelligence, 27 March 2013.*
[50] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[51] *Oral Evidence – Security Service, 17 January 2013.*
[52] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[53] *Oral Evidence – GCHQ, 31 January 2013.*

military operation. Last year we highlighted that, whilst defending the UK against attacks in cyberspace must be a priority, there are also significant opportunities which should be exploited in the interests of UK national security.[54] These more proactive cyber capabilities must be closely linked to cyber 'defence': the lessons learned from one can feed into planning for the other. ***.[55]

49. ***.

50. ***.[56]

51. ***.[57] ***.

52. A key focus for the Ministry of Defence (MOD) is to define exactly how it envisages using cyber capabilities during future military campaigns. We have been told that the MOD has developed a joint doctrine on cyber operations, which sets out how cyber activities integrate into military operations and the legal framework within which they could be used.

53. To assist with its development of cyber capabilities, we have been told that the MOD is hoping to recruit those with specialist skills into the Reserve Forces. The work they might do would have to be different from that traditionally undertaken by Reservists, as the Chief of Defence Intelligence explained:

> *Our intent is to go out to the young computer professionals and make them an offer to do something good for their country but which will not require them necessarily to be doing normal [Reservist] business… we're very much focused on the fact that these will not be people that will spend a lot of time running around ranges with rifles. We're going to offer them a different proposition, as it were, if they want to be in the Reserve cyber.*[58]

E. Whilst work is under way to develop those capabilities that will protect the UK's interests in cyberspace, it is now halfway through the Spending Review period, and we are therefore concerned that much of this work remains preparatory and theoretical, with few concrete advances.

Resourcing cyber security

54. We have seen increasing effort from all the Agencies on the cyber agenda. Although it is difficult to separate some of this work out from other areas (since cyber is increasingly a cross-cutting issue), for the first time the Agencies have presented us with figures showing the numbers of people involved in this work, and how it has increased over the last two years. As an example, SIS allocated *** full-time equivalent (FTE) members of staff to cyber work in 2012/13, and GCHQ now has *** working solely on cyber defence (the total extent of GCHQ's work on cyber is much greater, but is difficult to quantify as it is spread across most of its business).

---

[54] *These include the following: active defence; exploitation; disruption; information operations; and military effects. These are described in more detail in our 2011–2012 Annual Report.*

[55] *Oral Evidence – GCHQ, 31 January 2013.*

[56] *Oral Evidence – GCHQ, 31 January 2013.*

[57] *Oral Evidence – Defence Intelligence, 7 February 2013.*

[58] *Oral Evidence – Defence Intelligence, 7 February 2013.*

55. We have previously expressed our concerns over the ability of the Agencies (and in particular GCHQ) to attract and retain suitably qualified cyber specialists given the competition from the private sector. As the Director of GCHQ put it to us previously, "*[GCHQ] can offer them a fantastic mission, but… can't compete with their salaries*".[59] In a previous Annual Report, we recommended that the Government re-examine what could be done to encourage retention of these skilled individuals.[60] We have now been informed that GCHQ has implemented more flexible reward packages for internet specialists. Whilst it is too early to tell if this will solve GCHQ's problems with recruitment and retention of cyber specialists, the Director told us:

> *Feedback from, if you like, the opinion formers and some of the fiercest critics of the previous system… has been very positive. We have had a couple of people withdraw resignations. We've had other people who have been adamant that they would leave now saying that they will stay.*[61]

56. This is reassuring; however, he acknowledged that GCHQ would never be able to compete directly with private sector salaries, and that further work was needed to create a system that would make a real impact in this area:

> *I think we'll always have fewer of these people than we would like. I think we will recruit fewer than we would like… I think we will still lose people, but I think we'll have a much better pipeline of talent in. I think also we'll have a much better disposed staff. People will leave. People may come back. And one of the metrics for me is that people who we've already lost may now come back to us.*[62]

57. The scale of the UK's effort will need constantly to be reviewed against that not just of our adversaries but also our allies. Although the Foreign Secretary has told us that "*we are probably ahead of the vast majority of the world*"[63] in the progress that has been made, the resources being committed to countering the cyber threat by other countries are vast: the US announced earlier this year that it was recruiting a further 4,000 personnel into its cyber command,[64] and we have been told that ***.[65] Although we cannot hope to match the resources of the US, we must consider whether more resources are needed to provide a step-change in our cyber effort. The UK cannot afford to lag behind in building its cyber skills and capabilities.

58. We welcome the decision in the recent Spending Review to extend funding for the National Cyber Security Programme into 2015/16. Continued financial commitment to, and investment in, the full range of cyber capabilities is vital: it is clear that if work to counter the growing cyber threat is not adequately funded then the UK's security will be adversely affected. However, we note that the extension is only for one year.[66] In order to plan effectively, the Agencies will need assurances that this funding will continue beyond 2015/16 and, crucially, that it will be incorporated into the Agencies' budgets rather than kept as a separate funding stream. That said, we have also been concerned to hear reports of a debate at the heart of Government over whether funding for counter-terrorism should

---

[59] *Oral Evidence – GCHQ, 3 February 2011.*
[60] *Cm 8114.*
[61] *Oral Evidence – GCHQ, 31 January 2013.*
[62] *Oral Evidence – GCHQ, 31 January 2013.*
[63] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[64] *'Pentagon Expanding Cybersecurity Forces to Protect Networks Against Attacks', New York Times, 27 January 2013.*
[65] *Oral Evidence – GCHQ, 31 January 2013.*
[66] *No budgets or baselines beyond 2015/16 have yet been agreed.*

be reallocated to cyber security. There cannot be an 'either/or' approach to addressing these significant threats: both areas must be adequately resourced.

F. Cyber security will continue to be a significant threat beyond the end of this Spending Review period. We are pleased to see that the funding for the National Cyber Security Programme will be extended into 2015/16. However, planning must begin now to ensure that resources will be made available to combat cyber attacks in the latter half of this decade, bearing in mind the resources our allies are putting into this area in recognition of the seriousness of the threat. The Government must ensure that real progress is made as part of the wider National Cyber Security Strategy: the UK cannot afford not to keep pace with the cyber threat.

SECTION 6: COUNTER-PROLIFERATION

59. The UK remains actively engaged in international efforts to combat the proliferation of Weapons of Mass Destruction (WMD). Within the UK, an attack using chemical, biological, radiological or nuclear (CBRN) weapons is considered to be a Tier Two risk in the Government's National Security Strategy,[67] judged as being of low likelihood but having a very serious impact.

60. Whilst the Government continues to apply pressure and sanctions, and to engage diplomatically, the intelligence community has a distinct role to play in tackling the proliferation of these weapons both through intelligence-gathering to keep the Government informed about the state of WMD programmes and covert operations to disrupt those programmes. Counter-proliferation was a high priority for SIS in 2011/12, ***.

Intelligence on the Iranian nuclear programme

61. An Iranian nuclear weapons capability would further ignite tensions across the Middle East and threaten regional stability. ***.[68] ***, the Foreign Secretary emphasised that Iran is increasing its enrichment capacity, "*which has no plausible peaceful explanation*".[69]

62. Against this backdrop, we questioned what effect the international sanctions regime was having. The Foreign Secretary told us that it was "*having a big effect… [and] has helped to slow down the Iranian programme and extend the timelines. But such activity will not on its own stop the Iranian nuclear programme*".[70] The Chief of SIS explained that successfully preventing proliferation relies on co-ordination between the UK intelligence community and their international partners. This collaboration, led by the Inter-Agency Counter-Proliferation Joint Operations Centre, has resulted in ***.[71]

63. ***. The Foreign Secretary told us:

> *… we don't believe that while we are engaged in this process of sanctions and negotiations and a twin-track policy it would be right to launch a military strike on Iran and we've said that very clearly to the Israelis.*[72]

***.[73]

64. ***, we recognise that the Agencies are having to become more creative in how they maintain and develop accesses to supply the Government's intelligence requirements.[74]

G. The Committee recognises the significant contribution that the Agencies are making to the international efforts regarding Iran's nuclear weapons programme. Such work should continue to receive a high priority. However, we note the challenges posed in gathering intelligence against this particular target.

---

[67] *Cm 7953.*
[68] *Oral Evidence – SIS, 24 January 2013.*
[69] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[70] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[71] *Oral Evidence – SIS, 24 January 2013.*
[72] *Oral Evidence – Foreign Secretary, 22 November 2012.*
[73] *Oral Evidence – SIS, 24 January 2013.*
[74] *Written Evidence – SIS, 20 March 2013.*

Syria

65. The Syrian Government has not explicitly confirmed details of its chemical weapons capability although it has spoken, in hypothetical terms, about using such weapons to deter foreign invaders. There is no doubt amongst the UK intelligence community that the Syrian regime possesses vast stockpiles of these deadly weapons.

SYRIA'S CHEMICAL WEAPONS STOCKS

Open source assessments vary considerably, but suggest that Syria's stockpiles of chemical weapons include the following:

- Mustard gas (sulphur mustard): yellow or brown oily liquid which causes blisters and burns to the skin and, if inhaled, can damage the lungs. Symptoms may only emerge hours after exposure.
- Sarin: a clear, colourless liquid which attacks the central nervous system and can be spread as a gas or liquid; just a few drops on the skin can be fatal. It was used in a 1995 attack on the Tokyo underground system which killed 13 and injured over 1,000.
- Ricin: a highly toxic protein derived from the castor oil plant, ricin is poisonous if inhaled, injected or ingested; a few grains of this white powder can cause organ failure and death in a matter of days.
- VX: the deadliest nerve agent ever created, VX is a clear or amber-coloured oily liquid. A fraction of a drop absorbed through the skin can kill in minutes.

***.

66. In December 2012 the Foreign Secretary said that he had seen evidence that Syria was preparing to use its chemical weapons,[75] and in January 2013 SIS told us that "*the most worrying point about our intelligence on Syria's attitude to chemical weapons is how low a threshold they have for its use*."[76] Since then, there have been multiple reports in the media that sarin may have been used in small quantities against, and possibly by, Syrian opposition forces, and in June the US, UK and French governments said that they have high confidence that the Assad regime has used chemical weapons on a small scale.

67. The security of these chemical weapons stocks is also of serious concern. The Chief of SIS noted the risk of "*a highly worrying proliferation around the time of regime fall*."[77] There has to be a significant risk that some of the country's chemical weapons stockpile could fall into the hands of those with links to terrorism, in Syria or elsewhere in the region – if this happens, the consequences could be catastrophic. ***.[78]

[75] *'UK's Hague confirms 'evidence' of Syria chemical arms plans', BBC News, 8 December 2012.*
[76] *Oral Evidence – SIS, 24 January 2013.*
[77] *Oral Evidence – SIS, 24 January 2013.*
[78] *Oral Evidence – Foreign Secretary, 22 November 2012.*

North Korea

68. In December 2012 North Korea launched a missile which was reported to have successfully placed a satellite into orbit. Such a missile could, analysts claim, also double as an intercontinental ballistic missile carrying a nuclear warhead. Subsequently, in February 2013, North Korean state media announced a nuclear test – the country's third – using a "*miniaturised and lighter… device with greater explosive force than previously*".[79] In addition to their nuclear weapons programme, there are also concerns about North Korea's proliferation activities, and the possibility that nuclear material could fall into the hands of terrorists or non-state actors.

69. ***[80, 81], the Chief of SIS said:

> *Ultimately the test of success is [that] the North Koreans move progressively in a direction which makes them less of a threat to their neighbours and to the wider world, either from a military point of view or from a proliferation point of view.* ***.[82]

Pakistan

70. Concerns regarding the security of Pakistan's deployed strategic nuclear weapons have decreased, as the country has become more stable politically and the risk of the weapons falling into the hands of Al-Qaeda, the Taliban or groups such as Lashkar-e-Tayyaba has lessened. ***.[83]

Collaborative working: the 'virtual hub'

71. Counter-proliferation is an area where collaborative working is crucial in ensuring success. We reported last year that the Government had established a 'virtual hub' in Defence Intelligence, bringing together experts from across the intelligence community. We have been told that this hub, which provides analytical expertise for the range of issues relating to counter-proliferation work, is "*increasingly acknowledged as the centre of excellence within government for analysis on these complex issues, whether they're nuclear or chemical and biological*".[84] The hub's outputs are used as the basis for the UK's international engagement, supporting the drawing up and enforcement of international sanctions, which are coordinated by the Inter-Agency Counter-Proliferation Joint Operations Centre.

72. We were, however, concerned to be told this year that the hub was "*seeking strengthened governance and clearer priorities… within the framework of the National Counter-Proliferation Strategy*."[85] We questioned whether this meant that such governance and priorities had not been in place when the hub was first established. We were told that the pressures on the hub in terms of the number of international proliferators, combined with constrained resources across defence, meant that "*we've had to prioritise quite hard on what we move forward at the moment and what we put to one side for now and come back to another day… there has been a tension there between, if you like,*

[79] *'North Korea's nuclear tests', www.bbc.co.uk/news, 12 February 2013.*
[80] *Oral Evidence – GCHQ, 1 December 2011.*
[81] *Written Evidence – SIS, 9 September 2012.*
[82] *Oral Evidence – SIS, 24 January 2013.*
[83] *Oral Evidence – SIS, 24 January 2013.*
[84] *Oral Evidence – Defence Intelligence, 7 February 2013.*
[85] *Written Evidence – Defence Intelligence, 15 November 2012.*

building some of the structures around the hub and actually doing day to day work."[86] It is important that the good work that the hub has carried out to date is not eroded by poor governance arrangements or confusion over its priorities. Work to clarify these areas must be completed as a matter of urgency.

[86] *Oral Evidence – Defence Intelligence, 7 February 2013.*

SECTION 7: SUPPORT TO MILITARY OPERATIONS

73. The intelligence community, and Defence Intelligence (DI) (which is part of the MOD) in particular, provide support to a range of current or potential military operations by UK forces. Although the largest is the British military presence in Afghanistan, others include:

- support to Armed Forces deployments in the Gulf and Balkans;
- counter-piracy off the Horn of Africa;
- support to the nuclear deterrent;
- support to contingency operations such as hostage rescue operations; and
- monitoring any Argentine threat to the Falkland Islands.

This year we have examined in some detail the nature of this requirement and the challenges it presents for the three Agencies and DI.

Afghanistan

74. The UK maintains a significant military presence in Helmand province in Afghanistan, and the intelligence effort to support this remains considerable. DI describes the resource that it provides to this area as "*very significant*",[87] and the effort from GCHQ and SIS is also substantial: Afghanistan and Pakistan absorb around ***% of GCHQ's effort,[88] and SIS allocates ***% of its overall work to Afghanistan.

75. Between them, the Agencies and DI have established a range of complementary capabilities over the last decade. These include:

- detainee interrogation;
- ***;
- technical collection;
- provision of mapping information;
- analysis of imagery;
- all-source assessment on strategic, political and military topics and operational matters;
- training and mentoring vetted units of Afghan forces; and
- supporting improved governance and rule of law among Afghan institutions.

Collaborative working

76. There is considerable coordination and cooperation between the Agencies and DI in respect of their work supporting the military. This is particularly true of GCHQ, which funds some joint capabilities and activities where military skills and experience are necessary or where the location requires military support.

[87] *Written Evidence – Defence Intelligence, 15 November 2012.*

[88] *This includes GCHQ-funded military personnel who carry out work in support of GCHQ's priorities in the region; when these are removed, counter-terrorism remains the highest priority for GCHQ staff.*

77. DI and GCHQ closely coordinate their signals intelligence activities (including procurement of equipment, training and operational planning) to support military operations. DI has given the Committee examples of what can be achieved through such collaboration.

78. On the HUMINT (Human Intelligence) side, supporting military operations requires close working between DI and SIS, both to produce operational intelligence and to support the UK's programme of capacity building in Afghanistan. Although there is no agreement similar to that between DI and GCHQ, we understand that the Chief of Defence Intelligence is keen to work more closely with both SIS and the Security Service (and possibly the new National Crime Agency) to cooperate and share expertise, and to maintain the skills of DI's HUMINT personnel once the Afghan campaign is over.

Outputs

79. We have described in previous reports how the work of the Agencies and DI produces both strategic and tactical intelligence: this may range from assessments of the latest political developments to work countering Improvised Explosive Devices (IEDs) and protecting forces on the ground. We have taken further evidence this year on the range of results, which include:

- analysis of the IED threat, which DI assesses has "*saved lives and enhanced force protection*";[89]
- ***;
- as part of its mapping work, DI producing maps with Dari script to support the training of Afghan forces;
- ***;[90]
- SIS work in support of potential political reconciliation efforts;[91] and
- GCHQ disruption of "*multiple direct threats to UK forces and personnel*",[92] and the delivery of significant reporting ***.

Drawdown

80. On current plans, the UK will cease combat operations by the end of 2014, and the majority of UK forces will have been withdrawn. However, the Committee understands that final decisions on what forces might remain in a training and advisory role have yet to be made. This means that it is unclear what intelligence support will be required from the Agencies and DI beyond this date, although we understand they are all planning reductions in the numbers of personnel deployed in theatre and supporting the Afghanistan campaign from the UK. Aspects of the capacity building and mentoring task are expected to continue beyond 2014, ***.[93] Whilst this planning is sensible, the level of intelligence support required after the drawdown will need to be established soon if the Agencies are to be able to plan effectively.

---

[89] *Written Evidence – Defence Intelligence, 15 November 2012.*
[90] *Written Evidence – SIS, 11 September 2012; Written Evidence – GCHQ, 11 September 2012.*
[91] *Written Evidence – SIS, 11 September 2012.*
[92] *Written Evidence – GCHQ, 11 September 2012.*
[93] *Written Evidence – SIS, 20 March 2013.*

81. We questioned DI about the impact the drawdown would have on its resources, and in particular on the Defence HUMINT Organisation (DHO). We have previously reported on the delays in recruiting, training and deploying additional HUMINT personnel to Afghanistan: despite receiving approval in 2009 for an increase, it is only now – as the end of the campaign is approaching – that the bulk of this increase is being delivered. The Committee is concerned that, if these personnel are left without work after the withdrawal, at a time when the MOD is under considerable cost pressures, they may be an easy target to cut. This would mean the time and effort spent building up this capability would have been wasted and, in the event that a future conflict required similar skills, the same lengthy and expensive process of recruitment and training would need to be repeated.

82. The Chief of Defence Intelligence (CDI) acknowledged that there would need to be a review of the numbers of HUMINT personnel: he pointed out that "*we scaled this to do Afghanistan and Iraq at the same time. The challenge is: is that scale right for the future activity?*" However, he seemed confident that this important capability would be maintained:

> *… it's not a question of whether we will have the capability… I'm confident that those who are at the Defence Board level understand the time it's taken us to generate this capability and will not want to lose it… IEDs are a fact of life, in any form of future conflict. I'm confident that the [contribution of HUMINT personnel] as part of that counter-IED fight, let alone all of the other stuff that they do, is absolutely made and realised and recognised across Defence.*[94]

83. We understand that GCHQ is in discussion with the MOD about the future requirement for military skills and experience, ***.[95]

H. The support provided by the Agencies and Defence Intelligence to the UK's military operations in Afghanistan has been invaluable. We are, however, concerned that Defence Intelligence's intelligence collection capabilities, which have been built up slowly and at considerable cost to support the campaign, may be easy prey for a department looking to make financial savings. We urge the Government to ensure that these vital capabilities are preserved and to give consideration as to how they can be redeployed when not required in support of combat operations.

Resourcing

84. Aside from Afghanistan, the Agencies' and DI's support to the military encompasses a range of tasks, and additional demands are constantly emerging. For instance, as the Government's focus of the 'Arab Spring' has shifted from Libya to Syria, so have the resources being put into this area. More recently, we have seen events in such countries as Mali, where the UK is now providing limited military support, come to the fore. We note that the Prime Minister has suggested that the fight against terrorism in North Africa "*will require a response that is about years, even decades, rather than months*".[96] This will undoubtedly place further demands on the intelligence Agencies and DI in an area in which they might previously have expected not to devote much effort.

85. We discussed in our 2011–2012 Annual Report how the Agencies and DI responded to these challenges, shifting resources to cover the new demands at the expense of other

[94] *Oral Evidence – Defence Intelligence, 7 February 2013.*
[95] *Written Evidence – Defence Intelligence, 27 March 2013.*
[96] *'Update by the Prime Minister about Algeria', www.number10.gov.uk, 20 January 2013.*

areas. We further noted how, in DI's case, cuts to the MOD's budget will lead to the loss of 450 DI posts over the current Spending Review period – more than 10%.[97] We have been told this year that DI is continuing "*to take moderate risk*"[98] on some areas in order to resource higher priority areas. CDI also admitted to us that:

> *… we have had to take output reductions. You know, we've moved people off certain areas we're not able to give so much depth as we once were… The effect of that is quite difficult to quantify today because these things… are not about today's business… my worry, and it's an unquantifiable worry, is [the potential loss of] the longer term deep [analysis] and other technical intelligence that we were previously doing that may be an issue in a few years' time.*[99]

86. The Agencies and DI have attempted to minimise the impact of this by putting in place 'burden-sharing' agreements with our allies. For certain geographic areas or technical subjects where an ally may be better placed, the UK will rely on their intelligence to inform our assessment, policymaking or indeed military planning. Conversely, where the UK has areas of expertise, we will supply intelligence to other countries. Whilst the UK will not cease all intelligence collection and analysis on entire areas, it will mean the Agencies and DI can focus scarce resources where they can have most impact.

87. We accept the need for this specialisation. It is not novel: for example, we have been told that "*in [the recent campaign in] Libya we went to war on German maps*".[100] To be fully effective, however, it relies on a detailed understanding between countries of where each will concentrate, and the timely sharing of highly sensitive intelligence. (The importance of this emphasises the need for the UK to be a trusted intelligence partner: this has been of particular relevance to Parliament's consideration this year of the Justice and Security Act, on which we comment further on page 31.)

88. In addition, DI has told us that it has plans to 'surge' analysts (drawn either from its existing staff or identified Armed Forces personnel with the requisite skills) into areas such as Iran or Syria, should there be a requirement to do so. Whilst these plans appear prudent, we remain concerned that this may not leave DI sufficiently resilient should a number of crises emerge simultaneously, and that large areas may be left with reduced coverage.

I. The Committee has repeatedly warned of the risks of cutting resources – in particular to Defence Intelligence – to the UK's ability to provide the necessary level of global coverage. Whilst we recognise that burden-sharing arrangements with allies may offset some of the impact, there must continue to be a critical mass that can respond to unexpected events without this being at the expense of coverage of other key areas. We are concerned that shifting resources in response to emerging events is 'robbing Peter to pay Paul': we must maintain the ability to respond to more than one crisis at a time.

---

[97] *Defence Intelligence is mostly funded from the MOD's budget, which is being cut by 8% over the 2010 Spending Review period (April 2011 to March 2015).*

[98] *Written Evidence – Defence Intelligence, 14 September 2012.*

[99] *Oral Evidence – Defence Intelligence, 7 February 2013.*

[100] *Oral Evidence – Defence Intelligence, 7 February 2013.*

SECTION 8: WIDER INTELLIGENCE ISSUES

Legislation

Draft Communications Data Bill

89. Communications data refers to the 'who, where and when' of a communication, but not the content of what is being communicated. The ability of the intelligence and security Agencies to access communications data is critical to their ability to counter threats to the UK's national security – most notably the threat of terrorism.

90. In June 2012, the Government published a draft Communications Data Bill which was intended to modernise the existing arrangements for the Agencies and other public bodies to access this data. A Joint Committee of Parliament was established to conduct formal pre-legislative scrutiny of the draft Bill. It published its report[101] in December 2012. The ISC undertook a parallel investigation, concentrating on the use of communications data by the intelligence and security Agencies. The ISC's report was sent to the Prime Minister in November last year, and was published in February 2013.[102]

91. Both Committees recognised the need for the current arrangements governing access to communications data to be modernised, but were also critical of certain aspects. The ISC recommended that the draft Bill needed to be revised in terms of scope, and drafted more tightly in terms of the Government's proposed new powers. Whilst accessing communications data is one of the least intrusive ways the Agencies can investigate possible threats, it does nevertheless represent an intrusion into an individual's personal life and is therefore a serious matter. We concluded in our report that the Government needed to give more details on its proposals. The Joint Committee made similar recommendations. After considering the reports of both Committees, the Government agreed to rewrite the draft Bill and to undertake further consultation – particularly with the Communications Service Providers (another of our recommendations).

92. At the time of writing the revised Bill has not been introduced to Parliament, and the Government's intentions are unclear. We are concerned that not enough has been done to resolve this issue. The problem will not go away – there remains a capability gap in the ability of the police and Agencies to access communications data which must be addressed.

Justice and Security Act

93. In October 2011, the Government published its Justice and Security Green Paper, outlining improvements to the arrangements for parliamentary oversight of intelligence and security matters and proposing reforms for the handling of sensitive material in the civil courts. The Justice and Security Act received Royal Assent in April 2013.[103]

94. The ISC has supported the principle of making Closed Material Procedures (CMPs) available in civil proceedings. Although the system of open justice in this country is a fundamental principle, it is preferable that important evidence should be heard by a judge, rather than excluded altogether under the system of Public Interest Immunity (PII)

[101] *HC479/HL79.*
[102] *Cm 8514.*
[103] *Part 1 of the Act reforms the ISC: this is covered on page 45.*

certificates. Exclusion of evidence risks that one or both parties to proceedings will not receive a fair trial.

95. The proposals to introduce CMPs in the civil courts proved highly controversial. There were powerful arguments put forward both for accepting the status quo and for the Government's proposed reforms. As a result, the Government made a number of concessions, including accepting greater discretion for judges and ensuring that only national security sensitive material (rather than all 'sensitive' material) should be covered. However, the Committee remains concerned that the new provisions will not be available to use in inquests, even if a coroner wishes to use them.

96. A second important provision in the Act is the restriction on the use of the Norwich Pharmacal jurisdiction in relation to sensitive information, the disclosure of which would be damaging to national security or the UK's international relations. In recent years an increasing number of Norwich Pharmacal claims have been launched against the Government, by those seeking the release of intelligence material in support of legal action in other jurisdictions. In some cases, this material has been provided to the UK Agencies in confidence by their overseas intelligence partners. However, the judgment in the Binyam Mohamed case showed intelligence partners that the Government's PII claim that sensitive material should be protected from disclosure would not always be upheld, and in Norwich Pharmacal cases (where disclosure is the objective of the case), the Government then would have no option but to disclose. The disclosure of such material resulted in some of the UK's intelligence partners reviewing, and in some cases restricting, their intelligence-sharing arrangements with the UK. Such a situation could not be allowed to continue.

J. Closed Material Procedures allow evidence to be heard which, under Public Interest Immunity arrangements, was previously excluded from cases altogether (sometimes leading to the abandonment of proceedings and/or an unavoidable settlement if the Government could not bring evidence in its defence). While CMPs are not ideal, they are better than the alternatives: this is an imperfect solution, but a pragmatic one. Taken together with the Norwich Pharmacal reforms, we consider that the changes should allay the concerns of those allies with whom we exchange intelligence crucial to our national interest.

The Joint Intelligence Committee

97. In its Annual Report last year,[104] the Committee reported on the Cabinet Office review of the central intelligence machinery, including the work of the Joint Intelligence Committee (JIC). The review clarified the relationship between the JIC and the National Security Council (NSC), defining the JIC's role in responding to the NSC's requirements when producing assessments.

98. A new Chair of the JIC was appointed in March 2012. He began by undertaking a stock-take of JIC business, and recommended a detailed package of measures to strengthen the JIC's engagement with the rest of the intelligence community (which had appeared to be fading) and to ensure that the JIC remained central to Whitehall's decision-making. There had been concerns that the JIC was becoming irrelevant: in the JIC Chair's words,

[104] *Cm 8403.*

his changes were designed to ensure that the JIC remains "*relevant… respected… and right*".[105]

99. The changes included:

- improving support to No. 10 (to ensure all written intelligence is coordinated and better tailored to the Prime Minister's needs);
- creating closer cooperation between the timetables and staff of the NSC and the JIC;
- a new model for JIC meetings to ensure Agency Heads only attend discussions pitched at the right strategic level, where they can best add value;
- a rationalisation of the JIC's written work from seven products to three, to clarify the status of each type of paper:
  - JIC Assessments – assessment papers approved by the JIC itself, either in or out of committee;
  - Joint Intelligence Organisation (JIO) Intelligence Briefs – short-notice JIO assessments in response to intelligence or other information, and approved by the JIC Chair (or delegated authority);
  - JIO Intelligence Summaries – assessments produced periodically in response to streams of intelligence or other information, in concert with the rest of the intelligence community if possible but on the authority of the JIC Chair (or delegated authority);
- a focus on clearer presentation to make JIC and JIO papers more accessible to Ministers and senior officials;
- a pilot exercise to review key judgements from the JIC to assess in retrospect whether they proved to be right; and
- work to ensure the right balance of engagement and input from both the intelligence and policy communities.

100. This more flexible system should encourage greater intelligence community cooperation, and increased understanding and use of the JIC's advice. The JIC Chair said that he hoped a more focused input from the Agency Heads means that "*under this system we will stand a better chance of picking up these big strategic shifts*", such as the 'Arab Spring'.[106]

K. The Committee welcomes the real changes made by the new Joint Intelligence Committee Chair, which demonstrate an understanding of how the JIC should operate at the centre of the UK intelligence machinery. Continuous improvements such as these are vital in ensuring intelligence advice to Ministers remains relevant and can respond quickly to changing requirements. We hope that these measures will reinvigorate the JIC and give it a new lease of life.

---

[105] *Oral Evidence – Chair, Joint Intelligence Committee, 29 November 2012.*
[106] *Oral Evidence – Chair, Joint Intelligence Committee, 29 November 2012.*

SECTION 9: AGENCY EXPENDITURE

101. In 2011/12, the Single Intelligence Account (SIA) was approximately £2 billion.[107]

	2011/12	2012/13	2013/14	2014/15
Single Intelligence Account (£m)[108]	1,928	1,991	1,908	1,883
Cyber Security funding and Critical Capability Pool Funding (£m)[109]	70	95	171	123

Each Agency's actual expenditure in 2011/12 was as follows:

- GCHQ spent £***m (within 0.3% of its budget);
- the Security Service spent £***m (within 0.9% of its budget); and
- SIS spent £***m (within 0.8% of its budget).

102. This is the third year of the 2010 Spending Review (SR10) settlement. In our 2010–2011 Annual Report[110] we expressed concerns that the real-terms cut of approximately 11.3% in the SIA might have an impact on the ability of all three Agencies to maintain coverage of the threat. We noted that factors such as public sector pay constraints and procurement savings meant that, despite inflation, front-line capabilities were being protected.

103. The 2011/12 resource accounts for all three Agencies were certified by the Comptroller and Auditor General in June 2012. The National Audit Office's (NAO's) audits raised a number of financial management and accounting issues which needed to be addressed. The majority of these relate to adherence to accounting standards, but other issues of note raised by the auditors included:

- an SIS payment of several million pounds relating to an operation with a foreign intelligence service which was not adequately documented;
- spending in excess of Treasury limits on advertising and marketing (SIS exceeded these limits in one of their external recruitment campaigns, although retrospective approval was eventually obtained); and
- incorrect treatment of ongoing liabilities relating to agent payments (Security Service).

Work is under way to address these issues, and all three Agencies continue to make improvements to their financial systems and management, with the assistance of the NAO.

---

[107] *In addition to the Agencies' budgets, 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; there have also been reductions to the settlement following the Chancellor's Autumn and Main Budget Statement.*

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

[109] *Resource DEL plus Capital DEL.*

[110] *Cm 8403.*

Major projects

104. The Agencies continue to spend a significant proportion of their overall budgets on capital projects. These projects primarily relate to improvements to IT systems, communications equipment and accommodation. This year the NAO has assisted the Committee in scrutinising the Agencies' finances and administration, including undertaking a detailed review of each Agency's biggest capital projects.[111]

105. In general terms, and across all three Agencies, most capital projects are on track to deliver their main objectives within budget and on time. In their latest formal reviews[112] nearly all projects have been assessed as 'Green' (on target to succeed) or 'Amber' (some changes or improvements required). The following summarises the key findings of the NAO's review:[113]

- In GCHQ, most projects are delivering the required business benefits.[114] While forecast costs can sometimes vary substantially from initial plans (often due to changing mission requirements during the course of projects), taken as a whole there is a net underspend.
- SIS has a number of major IT, communications and infrastructure projects under way. Of their seven largest projects, two have been assessed as 'Amber' in formal gateway reviews. While there have been minor delays and some issues with the other projects they are, in general terms, making satisfactory progress.
- The Security Service has eight major projects under way, with half reviewed as 'Amber'. These ratings largely reflect projects running behind schedule: in several instances this is because projects were postponed to allow the Service to focus on the Olympics. In cost terms the projects, as a whole, are running to budget (with one project considerably over budget balanced by one considerably under budget).

106. The ISC has, for a number of years, taken a close interest in the SCOPE IT programme, led by the Cabinet Office. The programme sought to provide a secure IT system and connectivity between a number of government departments and agencies and was to be delivered in two phases. While the first of these was successfully delivered at the end of 2007, Phase 2 was beset by problems and eventually abandoned by the Cabinet Office in July 2008. While the Committee investigated this failure in some detail, we did not publish our findings whilst the parties involved were engaged in arbitration. These negotiations have now concluded and a settlement has been reached. We are therefore able to report on our findings, which are included at Annex B.

---

[111] *This review was based on data provided by the Agencies.*

[112] *Gateway Reviews are carried out as a series of assurance 'gates' where projects are independently assessed before key project milestones are met.*

[113] *This review was based on data provided by the Agencies.*

[114] *The Desktop project continues to face difficulties. This is an issue that we will return to in due course.*

Efficiencies and savings

107. In our 2011–2012 Annual Report[115] we reported the sizeable savings and efficiencies that the Agencies must secure during the SR10 period (2011/12 to 2014/15) if they are to remain within budget. These comprise:

- £***m to be saved by GCHQ;
- £***m to be saved by the Security Service;
- £***m to be saved by SIS; and
- a further £220m to be saved across the SIA through tri-Agency projects and collaborative working.

108. Although the Agencies have a good track record of delivering efficiency savings from within their own budgets, we expressed concern last year as to whether the very considerable savings required from tri-Agency programmes and collaborative working would be achieved. We recommended that urgent work was needed by the central SIA finance team to re-evaluate plans and assess the viability of the collaborative savings programme.

109. Given our concerns, this year the NAO has reviewed the status of both the individual and collaborative savings programmes, and we also tasked our own Investigator to undertake a review. This latter review was postponed at the request of the National Security Adviser (NSA) who, in August last year, advised that as "*the main corporate programmes are still at an early stage*"[116] this review would be better conducted once they had more detailed plans in place.

Individual Agency savings

110. Although the Agencies appear to be making good progress against their internal savings targets, the NAO recommended that the claimed savings figures needed to be subject to more rigorous analysis. They highlighted a number of issues, including:

- baselines were difficult to establish, or incorrect, leading to less confidence in claimed savings in some cases;
- savings were reported gross of costs – making it difficult to distinguish between real savings and those where changes may have led to net increased costs;
- in some cases there was insufficient verification or evaluation of claimed savings, and in others there were inaccuracies in the calculation of savings; and
- there were a high proportion of one-off savings rather than those which would deliver benefits year on year.

L. There does seem to be a question as to whether the claimed savings and efficiencies that the Agencies must secure during the Spending Review period are independently verifiable and/or sustainable. The Agencies must ensure that reported savings are real and sustainable. The individual Agency and central SIA finance

[115] *Cm 8455.*
[116] *Letter from the National Security Adviser, dated 29 August 2012.*

teams must work together to address the National Audit Office's findings and provide the necessary levels of assurance.

Collaborative savings

111. The Comprehensive Spending Review in 2010 emphasised the need for the Agencies to collaborate more, not only to make them more effective but also to secure financial savings. The Structural Reform Plan for the Agencies outlined that "*the SR10 settlement was hard-wired with challenging single agency and collaborative working efficiencies.*"[117] This included a savings target of £220m across the Spending Review period for collaborative working efficiencies in particular.

112. In our last Annual Report,[118] we assessed progress against this savings target, expressing our concern that the plans would only realise savings of £158m, leaving a shortfall of £62m against the target of £220m. As recently as April 2013, the Chief of SIS confirmed that the savings targets had already been taken from their budgets. He described the £220m as "*an arbitrary figure to identify a target for us, and we were slightly surprised as agencies when our target was then invested into SR10 and taken off our baseline on the expectation that we would [achieve] that*".[119]

113. Given that the £220m had been taken off the Agencies' budgets, this indicated that this was a net amount, not gross. However, an analysis conducted earlier this year by the NAO on behalf of the Committee suggested that this target is in fact being treated as a gross savings target and does not take account of the cost of the programmes:

> *A single savings approach was agreed by the Tri-Agency Board setting out how the collaborative savings target would be recorded and monitored. This set out a principle that the £220m savings target would be interpreted as a gross target and that whilst the cost of achieving the savings would be monitored, savings would not be reported on a net basis. The Agencies consider that this approach is in line with the settlement agreement with HM Treasury.*[120]

This was not what we had understood to be the case. Indeed, it is substantively different: given that gross savings do not take account of how much will be spent to achieve them, potentially very little actual savings may be realised.

114. What is of even more concern is the fact that if the £220m has already been taken off the Agencies' baseline, but the Agencies are now going to achieve real savings somewhere below that figure (and possibly considerably below), then that leaves the Agencies either with an overspend, facing cuts, or needing to find extra savings elsewhere. Unless additional funding has already been secured, then the Agencies may be faced with cutting front-line capabilities to remain within budget. In December 2012, we asked the NSA whether there was an agreement with HM Treasury to 'bail out' the Agencies because of the nature of their work. He said: "*I do not think that is the sense at all. I think the Agencies will accept that they have to take some of the strain, alongside the rest of the Government, in reaching the Government's reduction targets*".[121]

---

[117] *Letter from the Cabinet Office, 15 April 2011, enclosing the SIA Structural Reform Plan.*
[118] *Cm 8403.*
[119] *Oral Evidence – SIS, 25 April 2013.*
[120] *National Audit Office Briefing for the Committee on the Secret Intelligence Service 2011–12, January 2013; briefing based on information provided by the Agencies.*
[121] *Oral Evidence – National Security Adviser, 29 November 2012.*

115. This lack of clarity about the nature of the collaborative savings target generally is mirrored in the changing picture of the individual workstreams. Taking the Corporate Services Transformation Programme (CSTP), initially in September 2011 we were told that this would achieve savings of £***m.[122] Then, in December 2012, we were informed that CSTP would achieve savings of £***m (at that time this represented a significant proportion of the total savings required).[123] However, just four months later, in April 2013, we were informed that CSTP had been shut down, after the corporate services element of the programme had encountered significant problems.

116. We were told that the Agencies had been *"concerned about its costs and the delivery of benefits in the coming years*".[124] They reviewed the programme and took the decision to scale back significantly their ambitions in relation to other aspects. They explained "*the costs were high and the benefits were relatively remote*".[125] The £***m included, we are now told, £***m of procurement savings: this element will continue and is forecast to save £***m over the SR10 period. The remainder of the CSTP programme is being taken forward as the Collaborative Corporate Services (CCS) programme, and is forecast to save £***m per annum (from the final year of the SR10 period).

M. Whilst we are reassured that some of the savings envisaged under the Corporate Services Transformation Programme (CSTP) will be achieved by other means, we note that the Committee was not kept informed about these changes. Although this was acknowledged to be a high-risk programme, as late as December 2012 – when we last received information on the collaborative savings programme – there was no indication of the trouble CSTP was in, nor of the effort being put into procurement savings. Indeed, we were asked to postpone our own review of the programme. This failure to keep the Committee informed of significant matters within its remit is unacceptable.

117. We also remain concerned at the lack of progress in the other workstrands. GCHQ told us there are two other areas "*undershooting*" at the moment: both Joint Internet Age Capability and Mission Facing Applications,[126] where the Agencies had "*set a very ambitious [combined] target of £*** million, and we are not in that zone over the four years*".[127] Whilst this may have been due to the Agencies' need to focus on security arrangements for the Olympic and Paralympic Games during 2012, the net result is that two of the four main workstreams are not on target to deliver the savings needed to protect front-line services. While procurement is now forecasting savings above its original target and IT Shared Services is on track to deliver its targets in full, the Director of GCHQ told us: "*the net forecast at the moment is below £220 million and we are not happy that it is below £220 million, but this is something under strong governance*".[128]

---

[122] *CSTP aimed to develop the corporate and administrative processes of the Agencies by improving business processes, making services more streamlined and reducing the numbers of staff and systems required to deliver them. A key strand of the programme involved the development of a joint Shared Service organisation to deliver corporate services.*

[123] *National Audit Office Briefing for the Committee on the Secret Intelligence Service 2011–12, January 2013; briefing based on information provided by the Agencies.*

[124] *Joint letter from SIS, GCHQ and the Security Service, 17 April 2013.*

[125] *Oral Evidence – SIS, 25 April 2013.*

[126] *Mission Facing Applications (MFA) aims to develop new capabilities which can be used by more than one agency, thereby saving overall investment costs. Joint Internet Age Capability is a set of experiments to test the value of new types of inter-agency collaboration on analytics and plays a key role in identifying where the MFA should focus. As this report was being finalised, we were informed that these two workstreams were now being treated as a single strand.*

[127] *Oral Evidence – GCHQ, 25 April 2013.*

[128] *Oral Evidence – GCHQ, 25 April 2013.*

118. In addition to the misunderstanding over gross or net savings, and the continuing savings gap, a third point made by the NAO is on the timing of when savings will be made. Many of the savings are planned to be made in the later years of the SR period,[129] particularly in 2014/15. We have seen many examples of individual Agency projects relating to the delivery of complex systems slipping by many months (sometimes by a year or more). Such slippage is even more likely when it comes to tri-Agency projects, which are inevitably more complex and involve more difficult business and cultural change. We are therefore concerned that there is a substantial risk that a large proportion of the savings planned in 2014/15 may not be delivered on time.

119. Given the serious concerns about the collaborative savings programme, we have pushed the Agencies for a more detailed update on progress. We have now been provided (as of May 2013) with a letter detailing the latest plans and workstreams. This is still a complicated picture, but we have attempted to summarise the original and latest plans on collaborative savings in the following table:

Collaborative savings plans (as at September 2011)		**Collaborative savings plans (as at May 2013)**		
Workstreams	**SR10 target**	**Workstreams**	**SR10 target**	**Latest forecast**
IT Shared Services	£***m	IT Shared Services	£***m	£***m
Corporate Services Transformation Programme	£***m	Corporate Shared Services	£***m	£***m
		Procurement	£***m	£***m
Joint Internet Age Capability	£***m	Joint Internet Age Capability and Mission Facing Applications	£***m	£***m
Mission Facing Applications	£***m			
De-duplication/ workstream overlap	£***m	De-duplication/ workstream overlap	£***m	£***m
Total savings target	**£***m**	**Total savings**	**£220m**	**£161m**
		Shortfall of forecast savings versus target		**£59m**

In this latest written update to the Committee, the Director of GCHQ accepted that "*we clearly had not done a good enough job of keeping the Committee up to date with the entirety of our approach*".[130]

120. The Director of GCHQ acknowledged that it is "*essential that the agencies achieve these efficiency targets, if we are to live within our SR10 settlement and avoid having to make a reduction in investment in our intelligence capability to cope with any shortfall*".[131] On the basis of this latest evidence, we now understand there are two actions in hand to mitigate the risk of any shortfall in the collaborative savings programme – a renewed focus on Joint Internet Age Capability/Mission Facing Applications to drive further savings, and a reliance on the individual Agency savings programmes over-achieving against their

[129] *This is in line with the SR10 settlement profile set by the Treasury.*
[130] *Letter from the Director of GCHQ, dated 29 May 2013.*
[131] *Ibid.*

targets. The Committee does not have enough evidence to assess whether these actions are on track. While the Agencies have assured us that the individual savings programmes "*are already £***m ahead of plan*", it is not clear whether these extra savings are in addition to the forecast total or have simply been achieved sooner than expected.

N. We recognise that during the run-up to the Olympics operational requirements were, rightly, prioritised over efficiency savings but time is running out: we are already over halfway through the Spending Review period in which these savings must be found. It is essential that real and sustainable efficiencies are delivered if front-line capabilities are to be protected. More needs to be done urgently.

O. The Agencies have said that they are "*fairly confident*" that operational capabilities will be protected during the Spending Review period: given the surprising lack of clarity around the collaborative savings programme – an issue that has such far-reaching consequences – the Committee does not fully share their confidence.

Staffing

121. Staff numbers in both GCHQ and SIS have decreased slightly from those reported last year, reflecting the continued budgetary constraints imposed by the SR10. The Security Service saw a slight increase, in the main as part of its investment in cyber, but also to mitigate the impact of the introduction of TPIMs. There was also an increase in staff seconded or attached to the Service as part of the response to the Olympic and Paralympic Games in 2012; this latter group of staff have since left and no further growth is planned. Average staff numbers during the last three financial years are shown in the following table:[132]

	2009/10	**2010/11**	**2011/12**
GCHQ	6,485	6,361	6,132
Security Service	3,831	3,847	3,961
SIS	3,082	3,324	3,200

Diversity

122. Last year we reported our initial findings on the demographics of the Agencies' senior leadership grades, concluding that greater efforts must be made to ensure more diverse workforces. We recognise that the intelligence Agencies have cultural issues to overcome, with additional challenges in terms of security vetting and nationality rules, and that it will take time to address the lack of diversity across their organisations. Nevertheless, there are considerable business and operational benefits to be gained from a broader range of backgrounds and views being represented within any organisation, and the intelligence and security Agencies are no exception.

123. Indeed, it is arguably more important for the Agencies to be able to draw on the broad range of talent and skills that a diverse workforce can offer: greater diversity not only provides a competitive advantage (increasing innovation and creativity amongst employees, and improving staff motivation and efficiency), but is also vital in adequately

[132] *These figures represent the average number of full-time equivalent people working at the Agencies during the year. This includes permanent staff, secondees, military personnel and time-hire contractors. Staffing figures given in previous ISC annual reports were calculated on a different basis.*

addressing the wide range of challenges that the Agencies face. If all intelligence professionals are from similar backgrounds with similar characteristics, they may share 'unacknowledged biases' that circumscribe both the definition of problems and the search for solutions – increased diversity will lead to better responses to the range of threats that we face to our national security.

124. We have therefore been considering the position of each Agency in more detail this year, and have held meetings with staff from all three organisations to understand the potential obstacles to achieving more balanced and diverse workforces. Our initial findings suggest that while progress is being made, it is slow, and more needs to be done. The focus of the Committee's enquiries relate to issues which are often cited as problems in large organisations, such as equality of access to promotion opportunities and whether leadership and middle management efforts to promote diversity are sufficient.

125. We were pleased to see examples of initiatives the Agencies are implementing to remove some of these barriers – for example, GCHQ highlighted a flagship initiative in their Dyslexia and Dyspraxia Support Group, which carries out successful awareness campaigns and provides mentoring and practical support to individuals. SIS has increased awareness and training to try to ensure that there is no 'unconscious bias' in their recruitment and selection procedures. The Security Service has launched a number of initiatives to improve diversity and has set itself challenging targets to improve gender diversity. Positive programmes like these, which focus on the benefits greater inclusion and diversity can bring, are an exemplary approach. We are keen to see more progress along these lines, and will report further in due course.

SECTION 10: REFORM OF THE INTELLIGENCE AND SECURITY COMMITTEE

126. The Justice and Security Act 2013 strengthens the powers and independence of the ISC. The ISC becomes a statutory committee of Parliament, with greater authority to consider intelligence and security activities in the Agencies and across wider Government. Although the ISC's status has been changed, the most important reforms are the Committee's ability to oversee the operational activities of the Agencies and the power to require information rather than request it (subject to the ability to withhold information, which can now only be exercised at Secretary of State level).

127. The result of these changes is that the ISC will have greater access to information, including primary material held within the Agencies, and it will have increased research and analysis resources at its disposal – including staff working more closely with the Agencies and able to inspect primary material at the Agencies' premises – to ensure that the Committee receives the information it needs to carry out the necessary levels of scrutiny.

128. The ISC of Parliament will also report independently and directly to both Houses of Parliament and through them to the public. While the Prime Minister will, rightly, retain the right to redact sensitive material from our reports, the Committee itself will publish them.

129. One of our first acts as the new ISC of Parliament will be to publish a Memorandum of Understanding between the Committee and the Prime Minister that will include some of the detailed working arrangements governing the ISC's new powers and remit. Pending further discussions with the Government and Prime Minister, we expect to lay this document before both Houses of Parliament in the near future.

130. The ISC has performed a crucial oversight role over the last 18 years despite, for much of that time, working within a limited legislative framework and with far too few resources at its disposal. Over this period, the level of scrutiny undertaken has been transformed and we thank previous Chairs and Members for their diligence and hard work. The reforms in the Justice and Security Act will radically improve the ability of the ISC to oversee the work of the Agencies. The Agencies themselves recognise that the challenge and scrutiny provided by a more powerful and effective Committee are in their own interest and can assist in uncovering problems and improving their work. In addition, a more effective ISC will give Parliament and the public confidence that the intelligence and security Agencies are properly being held to account by an independent Committee.

131. Unlike other parts of Government, intelligence and security matters cannot be effectively scrutinised in Parliamentary debates, or by a normal departmental Select Committee, the media, academia or pressure groups. Only a body with powers to access highly classified information can fulfil such a role. The ISC itself proposed many of the reforms now contained in the Justice and Security Act and we are therefore pleased that the Government has accepted the vast majority of our recommendations. The changes will lead to much improved oversight of the UK intelligence community.

ISC resources

132. The ISC has, for the last 18 years, been provided with its annual budget by the Cabinet Office. This funding supports the Committee's work overseeing the administration, expenditure and policy of the three intelligence Agencies. The bulk of the money provides for the Committee's small independent secretariat (which comprises one member of staff from the Senior Civil Service, one fee-paid Investigator and seven staff below the SCS).

133. The Justice and Security Act makes the ISC a statutory committee of Parliament and our funding arrangements will need to be updated to take account of this. We expect that funding for the Committee's secure accommodation and related facilities will continue to be the responsibility of Government (since these costs are a result of security rules mandated by Government), although our staffing and administration budget is now expected to fall to Parliament.

134. The Act also broadens the remit of the Committee and strengthens the ISC's powers. The ISC of Parliament now has responsibility for oversight of intelligence and security operations and its remit is expanded to include formal responsibility for oversight of all intelligence and security activities of Government, including parts of the Cabinet Office, the Office for Security and Counter-Terrorism in the Home Office, and DI. Furthermore, there is now a greater requirement for the Committee to be provided with information and there will be new ways of working, including greater access to the Agencies and their records, to underpin this.

135. We note commitments from a number of Government Ministers that the new ISC of Parliament will be adequately funded. The reforms in the Justice and Security Act are significant: they must be properly resourced.

ANNEX A: AGENCY STRATEGIC OBJECTIVES

Security Service:

ASO 1	To frustrate the international terrorist threat.
ASO 2	To frustrate the Northern Ireland-related terrorist threat.
ASO 3	To prevent damage to the UK from hostile foreign activity and other covert state activity.
ASO 4	To frustrate the international proliferation of material or expertise relating to weapons of mass destruction.
ASO 5	To protect sensitive Government information and assets and the UK's critical national infrastructure.

GCHQ:

ASO 1	Continue to make a substantial contribution to delivery of the UK's Counter-Terrorism Strategy.
ASO 2	Provide sustained support to Defence.
ASO 3	Deliver an agile response to other priorities.
ASO 4	Deliver an integrated and enhanced security mission.

Secret Intelligence Service:

ASO 1	Deliver intelligence securely and shape events according to NSC priorities, including on: • counter-terrorism; • prosperity; • security; • support to military operations; • counter-proliferation; and • global instability.
ASO 2	Operate an agile secret network capable of gathering intelligence and delivering effects globally.

ANNEX B: SCOPE

136. The SCOPE programme was designed as a major inter-departmental IT change programme in order to enable information-sharing across the wider intelligence community. It was intended to be delivered in two phases:

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

137. After a two-year delay, Phase 1 was fully implemented in late 2007, and in January 2008 the Committee was assured that concerted efforts were being made to ensure successful and timely delivery of Phase 2. However, just three months later, as the Committee reported in its 2007–2008 Annual Report,[133] the decision had been taken to abandon SCOPE Phase 2. The Committee reported that it was appalled at what appeared to be a waste of tens of millions of pounds, and said that it would investigate the reasons for the failure. In its 2009–2010 Annual Report[134] the Committee noted that it had taken further evidence and was in a position to report its findings; however, since both parties remained engaged in a contractual dispute process[135] the Committee had been asked to postpone publishing further details until this process had been completed. A settlement has now been reached and therefore we can now report on our findings.

138. There are two main issues the Committee considered: the decision to abandon Phase 2, and the outcome of the contractual dispute process with the Phase 2 contractor. On the decision itself, we understand that after a large number of defects had been identified by the contractor at the end of 2007, the Cabinet Office entered into commercial negotiations with the contractor to try to find an acceptable solution.

139. While these negotiations were progressing, the Cabinet Office separately commissioned an 'informal review' of the status of the Phase 2 project, outside the regular cycle of Office of Government Commerce reviews. The informal review reported to the SCOPE Oversight Board in late April 2008. It suggested that the numerous defects were caused by fundamental design challenges connected to the complexity of the project and its security requirements. It recommended that Phase 2 should be abandoned, as there was little prospect of successful delivery within any acceptable timescale or budget. Following this report, and after having taken technical, commercial and legal advice, the Cabinet Office decided to abandon the contract for SCOPE Phase 2 on 18 July 2008.

140. The Committee has heard additional evidence suggesting that this decision may have been taken too quickly. Dr Michael Taylor, Director of the SCOPE programme from 2001 until May 2008, is of the opinion that the success of Phase 1 was the result of strong backing from senior leadership, but that a weakening of the established governance procedures in late 2007 caused confusion thereafter. Dr Taylor highlighted that the 'informal review' of Phase 2 had been led by a civil servant inexperienced in delivering

[133] *Cm 7542.*
[134] *Cm 7844.*
[135] *The Cabinet Office informed the Committee in October 2009 that mediation had taken place in September 2009 which had failed to produce a resolution, ***.*

IT-enabled change programmes, and that the review did not appear to follow best practice. There is therefore a question over whether there was sufficient management buy-in after late 2007, and whether there was the will to see the project succeed. Nonetheless it is clear that the proposed solution by the contractor was not acceptable.

141. Following the project's cancellation, the Cabinet Office entered into a dispute resolution process with the contractor ***.

142. ***.[136]

P. Whilst SCOPE Phase 1 was successful, Phase 2 was beset by problems and delays and it is disappointing that it was abandoned. The strict security requirements led to a complex, highly customised secure solution which greatly increased the risk of the project failing. This must be borne in mind, and lessons learned, for future secure IT projects.

Q. The decision to cancel SCOPE Phase 2 was taken after an 'informal review' outside the normal governance arrangements, reducing accountability and inevitably raising questions over due process. It has since taken three and a half years to bring the Phase 2 project to a close. Whilst the details of the resolution are commercially confidential, we are aware of them and believe this represents a sensible conclusion to what has been a rather sorry saga.

[136] *Letter from the Minister for the Cabinet Office and Paymaster General, 14 November 2012.*

LIST OF RECOMMENDATIONS AND CONCLUSIONS

A. Despite the increased profile of other threats such as cyber security, counter-terrorism work rightly remains the primary focus of the intelligence and security Agencies. Their work in analysing intelligence to understand the threat and seeking to help to prevent attacks remains crucial to our national security.

B. The shape of the terrorist threat is potentially changing from tightly organised cells under the control of structured hierarchies to looser networks of small groups and individuals who operate more independently. It is essential that the Agencies continue to make a clear assessment of this evolving picture in order to keep ahead of the threat and to help to prevent attacks and loss of life.

C. The Committee shares the concerns of the Independent Reviewer of Terrorism Legislation over what happens when individual Terrorism Prevention and Investigation Measures (TPIMs) come to the end of their two-year limit. The Government must take steps now to ensure that they have sufficient policies in place when TPIMs have reached their limit and cannot be extended.

D. The threat the UK is facing from cyber attacks is disturbing in its scale and complexity. The theft of intellectual property, personal details and classified information causes significant harm, both financial and non-financial. It is incumbent on everyone – individuals, companies and the Government – to take responsibility for their own cyber security. We support the Government's efforts to raise awareness and, more importantly, our nation's defences.

E. Whilst work is under way to develop those capabilities that will protect the UK's interests in cyberspace, it is now halfway through the Spending Review period, and we are therefore concerned that much of this work remains preparatory and theoretical, with few concrete advances.

F. Cyber security will continue to be a significant threat beyond the end of this Spending Review period. We are pleased to see that the funding for the National Cyber Security Programme will be extended into 2015/16. However, planning must begin now to ensure that resources will be made available to combat cyber attacks in the latter half of this decade, bearing in mind the resources our allies are putting into this area in recognition of the seriousness of the threat. The Government must ensure that real progress is made as part of the wider National Cyber Security Strategy: the UK cannot afford not to keep pace with the cyber threat.

G. The Committee recognises the significant contribution that the Agencies are making to the international efforts regarding Iran's nuclear weapons programme. Such work should continue to receive a high priority. However, we note the challenges posed in gathering intelligence against this particular target.

H. The support provided by the Agencies and Defence Intelligence to the UK's military operations in Afghanistan has been invaluable. We are, however, concerned that Defence Intelligence's intelligence collection capabilities, which have been built up slowly and at considerable cost to support the campaign, may be easy prey for a department looking to make financial savings. We urge the Government to ensure that these vital capabilities are

preserved and to give consideration as to how they can be redeployed when not required in support of combat operations.

I. The Committee has repeatedly warned of the risks of cutting resources – in particular to Defence Intelligence – to the UK's ability to provide the necessary level of global coverage. Whilst we recognise that burden-sharing arrangements with allies may offset some of the impact, there must continue to be a critical mass that can respond to unexpected events without this being at the expense of coverage of other key areas. We are concerned that shifting resources in response to emerging events is 'robbing Peter to pay Paul': we must maintain the ability to respond to more than one crisis at a time.

J. Closed Material Procedures allow evidence to be heard which, under Public Interest Immunity arrangements, was previously excluded from cases altogether (sometimes leading to the abandonment of proceedings and/or an unavoidable settlement if the Government could not bring evidence in its defence). While CMPs are not ideal, they are better than the alternatives: this is an imperfect solution, but a pragmatic one. Taken together with the Norwich Pharmacal reforms, we consider that the changes should allay the concerns of those allies with whom we exchange intelligence crucial to our national interest.

K. The Committee welcomes the real changes made by the new Joint Intelligence Committee Chair, which demonstrate an understanding of how the JIC should operate at the centre of the UK intelligence machinery. Continuous improvements such as these are vital in ensuring intelligence advice to Ministers remains relevant and can respond quickly to changing requirements. We hope that these measures will reinvigorate the JIC and give it a new lease of life.

L. There does seem to be a question as to whether the claimed savings and efficiencies that the Agencies must secure during the Spending Review period are independently verifiable and/or sustainable. The Agencies must ensure that reported savings are real and sustainable. The individual Agency and central SIA finance teams must work together to address the National Audit Office's findings and provide the necessary levels of assurance.

M. Whilst we are reassured that some of the savings envisaged under the Corporate Services Transformation Programme (CSTP) will be achieved by other means, we note that the Committee was not kept informed about these changes. Although this was acknowledged to be a high-risk programme, as late as December 2012 – when we last received information on the collaborative savings programme – there was no indication of the trouble CSTP was in, nor of the effort being put into procurement savings. Indeed, we were asked to postpone our own review of the programme. This failure to keep the Committee informed of significant matters within its remit is unacceptable.

N. We recognise that during the run-up to the Olympics operational requirements were, rightly, prioritised over efficiency savings but time is running out: we are already over halfway through the Spending Review period in which these savings must be found. It is essential that real and sustainable efficiencies are delivered if front-line capabilities are to be protected. More needs to be done urgently.

O. The Agencies have said that they are "*fairly confident*" that operational capabilities will be protected during the Spending Review period: given the surprising lack of

clarity around the collaborative savings programme – an issue that has such far-reaching consequences – the Committee does not fully share their confidence.

P. Whilst SCOPE Phase 1 was successful, Phase 2 was beset by problems and delays and it is disappointing that it was abandoned. The strict security requirements led to a complex, highly customised secure solution which greatly increased the risk of the project failing. This must be borne in mind, and lessons learned, for future secure IT projects.

Q. The decision to cancel SCOPE Phase 2 was taken after an 'informal review' outside the normal governance arrangements, reducing accountability and inevitably raising questions over due process. It has since taken three and a half years to bring the Phase 2 project to a close. Whilst the details of the resolution are commercially confidential, we are aware of them and believe this represents a sensible conclusion to what has been a rather sorry saga.

GLOSSARY

AMISOM	African Union Mission in Somalia
ANF	Al-Nusrah Front
AQAP	Al-Qaeda in the Arabian Peninsula
AQI	Al-Qaeda in Iraq
AQM	Al-Qaeda in the Maghreb
ASO	Agency Strategic Objective
CBRN	Chemical, Biological, Radiological or Nuclear
CSS	Collaborative Corporate Services
CDI	Chief of Defence Intelligence
CESG	Communications-Electronics Security Group
CMP	Closed Material Procedure
CPNI	Centre for the Protection of National Infrastructure
CSTP	Corporate Services Transformation Programme
DHO	Defence Human Intelligence (HUMINT) Organisation
DI	Defence Intelligence
FATA	Federally Administered Tribal Areas
FTE	Full-Time Equivalent
GCHQ	Government Communications Headquarters
HUMINT	Human Intelligence
ICT	International Counter-Terrorism
IED	Improvised Explosive Device
IRA	Irish Republican Army
ISC	Intelligence and Security Committee
IT	Information Technology

JCHR	Joint Committee on Human Rights
JIC	Joint Intelligence Committee
JIO	Joint Intelligence Organisation
JTAC	Joint Terrorism Analysis Centre
MI5	Security Service
MI6	Secret Intelligence Service
MOD	Ministry of Defence
MP	Member of Parliament
NAO	National Audit Office
NSA	National Security Adviser
NSC	National Security Council
PII	Public Interest Immunity
PSNI	Police Service of Northern Ireland
RIRA	Real Irish Republican Army
SCOPE	Inter-departmental IT change programme
SIA	Single Intelligence Account
SIS	Secret Intelligence Service
SOCA	Serious Organised Crime Agency
SR	Spending Review
TPIM	Terrorism Prevention and Investigation Measure
WMD	Weapons of Mass Destruction

LIST OF WITNESSES

Ministers

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

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

Commissioners and Tribunal

The Rt. Hon. Sir Anthony May – Interception of Communications Commissioner (January 2013 onwards)

The Rt. Hon. Sir Paul Kennedy – Interception of Communications Commissioner (until December 2012)

The Rt. Hon. Sir Mark Waller – Intelligence Services Commissioner

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

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Sir Iain Lobban KCMG CB – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Sir John Sawers KCMG – Chief, SIS

Other officials

SECURITY SERVICE

Sir Jonathan Evans – Director General, Security Service (until April 2013)

Mr Andrew Parker – Director General, Security Service (April 2013 onwards)

Other officials

DEFENCE INTELLIGENCE

Vice Admiral Alan Richards RN – Chief of Defence Intelligence

Other officials

CABINET OFFICE

Sir Kim Darroch KCMG – National Security Adviser

Mr Jon Day – Chair, Joint Intelligence Committee

Other officials