Intelligence and Security Committee of Parliament

Annual Report 2016–2017

Chair:
The Rt. Hon. Dominic Grieve QC MP

Presented to Parliament pursuant to sections 2 and 3 of the Justice and Security Act 2013
Ordered by the House of Commons to be printed on 20 December 2017

HC 655

This publication is available at isc.independent.gov.uk

Any enquiries regarding this publication should be sent to us via our webform at isc.independent.gov.uk/contact

ISBN 978-1-5286-0168-9

CCS1217631642 12/17

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the APS Group on behalf of the Controller of
Her Majesty's Stationery Office

THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

This Report reflects the work of the previous Committee,[1] which sat from September 2015 to May 2017:

The Rt. Hon. Dominic Grieve QC MP (Chair)

The Rt. Hon. Richard Benyon MP (from 21 October 2016)	*The Most Hon. the Marquess of Lothian QC PC*
The Rt. Hon. Sir Alan Duncan KCMG MP (until 17 July 2016)	*The Rt. Hon. Fiona Mactaggart MP*
The Rt. Hon. David Hanson MP (from 21 October 2016)	*The Rt. Hon. Angus Robertson MP*
The Rt. Hon. George Howarth MP (until 18 October 2016)	*The Rt. Hon. Keith Simpson MP*
The Rt. Hon. the Lord Janvrin GCB GCVO QSO	*The Rt. Hon. Gisela Stuart MP*

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 was reformed, and its powers reinforced, 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 (SIS) 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 Agencies, officials from the intelligence community, and other witnesses as required. The Committee is supported in its work by a Secretariat. It also has access to legal, technical and financial expertise where necessary.

The Committee makes an Annual Report to Parliament 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

[1] *The following Members were appointed to the Committee in November 2017: the Rt. Hon. Dominic Grieve QC MP (Chair), the Rt. Hon. Richard Benyon MP, the Rt. Hon. the Lord Janvrin GCB GCVO QSO, the Rt. Hon. Ian Blackford MP, Kevan Jones MP, the Rt. Hon. Caroline Flint MP, the Most Hon. the Marquess of Lothian QC PC, the Rt. Hon. David Hanson MP and the Rt. Hon. Keith Simpson MP.*

security Agencies may request the redaction of material in the Report if its publication would damage their work, for example by revealing their targets, methods, sources or operational capabilities. The Committee considers these requests for redaction carefully. 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 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. This means that the published Report is the same as the classified version sent to the Prime Minister (albeit with redactions). The Committee also prepares from time to time wholly confidential reports which it submits to the Prime Minister.

CONTENTS

SECTION 1: THE WORK OF THE COMMITTEE

1. This Report details the work of the Intelligence and Security Committee of Parliament (ISC) for the period covering July 2016 to April 2017. During this time, the Committee has:

- held 21 full Committee meetings which have included 19 formal evidence sessions with, amongst others, the Foreign and Home Secretaries, the former National Security Adviser, the three intelligence Agencies,[2] Defence Intelligence and the Acting Chair of the Joint Intelligence Committee;
- held 20 other meetings;
- visited the Agencies and other parts of the intelligence community for briefings on six occasions;
- held bilateral discussions with those in the American, Canadian and French intelligence communities; and
- hosted delegations from Australia, Canada, Jordan, Pakistan and the USA.

2. This Annual Report was agreed by the previous Committee prior to the dissolution of Parliament in May. Major events since then have been noted in the text, but will be covered substantively in subsequent Reports.[3]

3. In addition to the work of the three intelligence and security Agencies and the wider intelligence community,[4] which is the subject of this Report, we have also published a report on *UK Lethal Drone Strikes in Syria*.[5]

The Investigatory Powers Act

4. In our last Annual Report we detailed our work on the Investigatory Powers Bill. This built on our earlier reports, *Privacy and Security: A modern and transparent legal framework* (published in March 2015) and *Report on the draft Investigatory Powers Bill* (published in February 2016).

5. The Bill was introduced to Parliament in March 2016. As the Bill progressed, we tabled a significant number of amendments, starting with 21 individual amendments at report stage in the House of Commons. In the House of Lords we tabled nine amendments at committee stage and three at report stage. The Government accepted a significant number of this Committee's amendments, which greatly improved what is now the Investigatory Powers Act. Chief amongst these were:

- the inclusion of a general privacy safeguard in section 1 of the Act, and a requirement that the Investigatory Powers Commissioner must specifically keep under review the operation of safeguards to protect privacy;

---

[2] *MI5, the Secret Intelligence Service (SIS) and the Government Communications Headquarters (GCHQ).*
[3] *The majority of this Report reflects the position as at 27 April 2017, when the Committee agreed the text of the Report. In certain cases we have noted subsequent events, primarily the terrorist attacks which have taken place since then; these will, however, be the subject of a further Report. We have also provided the most up-to-date Agencies' assessment of the threat in Section 2.*
[4] *Defence Intelligence (DI), the National Security Secretariat (NSS), the Joint Intelligence Organisation (JIO) and the Office for Security and Counter-Terrorism (OSCT).*
[5] *HC 1152, 26 April 2017.*

- greater independent oversight for warrants which allow intrusive activities against a group of people, as opposed to named individuals (known as 'thematic warrants'); and
- disallowing the use of a class Bulk Personal Dataset warrant in relation to a dataset containing a substantial proportion of sensitive personal data.

6. We also worked closely with a former Member of the Committee, Lord Butler of Brockwell, when he proposed amendments to make the abuse of bulk powers an offence under the Act (this was a fall-back solution in the event that the ISC proposal for an overarching offence did not proceed into law).

7. The Investigatory Powers Act achieved Royal Assent on 29 November 2016, following what amounted to a year's sustained engagement from the Committee. The Act represents a significant step forward in the transparency and governance of the Agencies' intrusive powers.

Diversity in the Agencies

8. We have reported previously on the demographics of the Agencies, concluding that at senior levels, in particular, they are not gender-balanced and do not fully reflect the ethnic make-up of modern Britain. In previous Annual Reports, the Committee called for greater efforts to be made to ensure more diverse and inclusive workforces; not only should the Agencies reflect the diversity of the UK as a matter of principle, but the Committee is confident that increased diversity will lead to better responses to the range of threats to our national security that we face.

9. There are significant 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 community are no exception. Indeed, it is arguably more important for the intelligence and security community to be able to draw upon the broadest range of talent and skills in the country; greater diversity not only provides a competitive advantage (increasing innovation and creativity amongst employees, and improving staff motivation and efficiency), but it also provides greater operational capability. In addition, if all staff are from similar backgrounds with similar characteristics, they may share 'unconscious biases' that circumscribe both the definition of problems and the search for solutions – heightening the risk of 'groupthink'.

10. The Committee recognises that the intelligence and security community has particular challenges in terms of security vetting and nationality rules, and that these are often the subject of myths and inaccurate perceptions about how they operate and the type of staff they recruit.

11. The Agencies have made genuine progress on diversity and inclusion issues over the last few years, but there is still further to go, particularly in relation to the collection of robust data against which to measure their progress.

12. Over the past nine months, the Committee has therefore been considering diversity and inclusion in detail within each of the organisations that fall within its remit. This work was led by the Rt. Hon. Fiona Mactaggart MP prior to the dissolution of Parliament on 3 May 2017. Ms Mactaggart wrote to the National Security Adviser on 27 April 2017 with

her initial findings. We hope the next Committee will build on her excellent work and publish a full report in due course.

Committee resources

13. The Committee is currently supported in its work by a team of seven core staff and seven Detainee Inquiry staff. The Committee's core budget of £1.3m was agreed by the Prime Minister in 2013. This excludes security, IT, telecoms, report publication, accommodation, utilities and centrally provided corporate services, which remain the responsibility of the National Security Secretariat (security expenses) and the Cabinet Office (other costs).[6] These costs were due to be transferred to the Committee's budget during 2016/17, but subsequently took place in 2017/18.

[6] *The budget has been fixed at this level to allow for the Committee to run two major investigations or inquiries simultaneously. When the ISC's Detainee Inquiry was established, the Cabinet Secretary and Ministers agreed that it should be funded at HMG expense. As a consequence, the ISC Secretariat was able to secure significant savings in the 2016/17 financial year – returning approximately one-third of its core budget to the Cabinet Office.*

SECTION 2: AGENCIES' ASSESSMENT OF THE THREAT

14. The threat to the UK and its interests overseas comes from a number of different sources, as outlined in previous Annual Reports, including international and Northern Ireland-related terrorism, Hostile State 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.[7]

The current threat picture

The threat to the UK from international terrorism

The threat from international terrorism in the UK is currently SEVERE – reflecting that an attack is highly likely. In 2017, between 23 and 26 May, the UK threat level was briefly raised to CRITICAL (an attack is expected imminently) for the first time since 2007, following the improvised explosive device (IED) attack on Manchester Arena.

The scale of the current threat facing the UK and its interests from Islamist terror groups is unprecedented. This threat is predominantly driven by the activities of Daesh (ISIL) in Syria and Iraq, which seeks to maintain the group's image and narrative of success in the face of military losses. Daesh still retains territory in Syria, Iraq and other ungoverned regions and continues to maintain its ability to project an external threat to the West through the prioritisation of so-called 'external operations' and the incitement of violence through extremist propaganda campaigns.

These threats have been realised in the form of three successful terror attacks and several disrupted attack plots since the start of March 2017. These events form part of a marked shift in the nature and extent of extremist attack planning activity, resulting in a reciprocal increase in the tempo of MI5 investigations.

Daesh's extremist narrative still has traction with the group's supporters globally. By using divisive sectarian messaging and grievances to justify its narrative, Daesh has emerged as the main extremist ideology responsible for radicalisation and the incitement of terrorism in the UK.

Al-Qaeda (AQ) also remains a persistent terrorist organisation with global reach. Whilst AQ's senior leadership has similarly been subjected to extensive pressure from counter-terrorism operations in recent years, degrading its capabilities and limiting its opportunities to plan attacks, the group remains a threat to Western interests.

The threat to the UK is diverse, as terrorist groups continue to innovate and employ a range of tactics, ranging from simple, low-sophistication attacks, such as those involving bladed weapons or vehicles, through to sophisticated, long-term attack plans involving the acquisition of IEDs.

[7] *Assessments of the level and nature of the threat from international terrorism are made by the Joint Terrorism Analysis Centre (JTAC); MI5 is responsible for setting the threat levels from Northern Ireland-related terrorism and other domestic terrorism, with separate threat levels being set 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).*

Alongside the direct threat from attacks, extremists within the UK continue to conduct other activities of national security concern in support of overseas Islamist groups. This includes those planning to travel to Syria and other conflict zones, individuals providing financial support for proscribed groups and those involved in disseminating Islamist messaging both in person and through the sharing of extremist media.

Northern Ireland-related terrorism

There is a persistent threat of terrorism in Northern Ireland (NI), primarily emanating from a small number of dissident republican (DR) groups who are opposed to the political process and remain committed to violence. The 'new IRA' is currently the most widespread and capable of the DR groups. It has carried out some of the most significant attacks in NI since it formed in 2012. Óglaigh na hÉireann has been rebuilding after a series of disruptions to its leadership while the Continuity IRA and Arm na Poblachta present more localised threats.

The threat level in NI remains at SEVERE (an attack is highly likely) while the NI-related terrorist threat to the rest of the UK was raised in May 2016 to SUBSTANTIAL (an attack is a strong possibility). DR groups continue to target and attack Police Service of Northern Ireland (PSNI) officers, prison officers and members of the armed forces. There were four attacks in 2016. This was an unusually low number (there were 30 in 2013, 22 in 2014 and 16 in 2015), attributed in part to security force pressure. However, in March the 'new IRA' deployed an under-vehicle IED which killed prison officer Adrian Ismay. This was the first fatality resulting from an attack since 2012, when the 'new IRA' shot and killed prison officer David Black. There have been four attacks in 2017 so far, including the non-fatal shooting of an on-duty PSNI officer by the 'new IRA'. These attacks demonstrate continued intent and the potential lethality of the threat in NI.

Hostile State Activity

The threat to the UK from espionage is both extensive and enduring. The UK continues to be a high-priority target for a number of hostile foreign intelligence services. Hostile foreign intelligence services continue to conduct espionage against a broad range of UK interests, seeking to obtain government and military secrets, intellectual property and economic information, and to conduct operations designed to influence UK policy and public opinion. They engage in a wide range of activity, encompassing the recruitment of human agents with the ability to acquire sensitive information (both protectively marked and unclassified) and, increasingly, the use of cyber in order to target the British Government, the UK's Critical National Infrastructure (CNI) and UK businesses.

The cyber threat

Cyber threats fall broadly into two categories – information/data theft and disruptive attacks. They can be conducted by a range of actors, from hostile states to criminals. The sophistication, complexity and potential impact of a cyber attack will vary depending on the level of access the actor has to resources and technology. A state actor may seek to integrate encryption and anonymisation into malware to penetrate a strategic target undetected. More commonly, far less sophisticated malware can be developed to target networks and systems to steal data. Systems are also vulnerable to insider threat, whereby the operator either knowingly or unknowingly facilitates access.

State actors or terrorists may have the desire to denigrate or disrupt an adversary's CNI but this would require a high level of sophistication. Criminals, including terrorists and

'hacktivists', may seek to disrupt websites through Denial of Service attacks either for publicity or to inflict reputational damage. They may seek to deface websites or redirect individuals to specific content in order to impart a particular message (e.g. extremist media or propaganda).

There is additionally the threat from cyber criminals, where the nature of the threat to the UK is diversifying: highly skilled actors are becoming increasingly competent and targeted in their attacks, whilst the barriers to entry for less-skilled actors are lowering. The aim, predominantly, is identify theft, fraud and extortion, whether through distributed denial of service attacks, ransomware or data extortion.[8]

Proliferation of weapons of mass destruction (WMD)

The UK continues to support international efforts to prevent WMD proliferation. Departments across Whitehall continue to work to counter the procurement of WMD-related equipment and materials from UK or international companies.

[8] *Data extortionists compromise and exfiltrate data, and then threaten to sell or release it unless a payment is made. In this way, data extortion differs from 'ransomware', which merely renders data unusable unless a ransom is paid. Organisations holding sensitive information such as patient records or financial information are particularly tempting targets for criminals, because they are more likely to pay to avoid disclosure and reputational damage.*

SECTION 3: INTERNATIONAL COUNTER-TERRORISM

15. Countering the threat of terrorism remains the primary focus for the intelligence and security Agencies (and indeed for all the organisations overseen by the ISC). In 2015/16, MI5 allocated 64% of its overall resources to International Counter-Terrorism work, with SIS and GCHQ allocating around a third and a quarter respectively.

16. The past year has seen the first fatal terrorist attacks occur within Britain since the murder of Fusilier Lee Rigby in May 2013. On 22 March 2017, a vehicle and knife attack took place in Westminster, killing five people. This was followed on 22 May by the bombing of the Manchester Arena, killing 22 people, and on 3 June by another vehicle and knife attack at London Bridge, killing eight people. In apparent 'retaliation' for these attacks, on 19 June a far-right terrorist launched a vehicle attack in Finsbury Park, London, killing one person. On 15 September, a bomb partially exploded on a train at Parsons Green, London, injuring numerous people. Our thoughts are with all those affected by this succession of tragic events. We also commend the bravery of PC Keith Palmer, who died defending others in the Westminster attack, and the many others who showed great bravery and resilience in resisting these attacks and assisting the victims.

17. There has also been a marked increase in the number of terrorist attacks elsewhere in Europe over the past two years. This has included a coordinated firearms attack in Paris, bomb attacks in Belgium, and the use of lorries as weapons of terror on the streets of Nice, Stockholm, Barcelona and at a Berlin Christmas market.

Terrorist attacks in Western Europe [9]

On 13 November 2015, Paris was the target of a coordinated terrorist firearms attack which resulted in 130 fatalities and was claimed by Daesh. The majority of the attackers were French or Belgian citizens with previous links to terrorism, although two were Iraqi. The French Prime Minister claimed that several of the killers had exploited migrant flows to 'slip in' unnoticed.[10]

On 22 March 2016, three coordinated suicide bombings took place in Brussels, targeting the airport and the Maalbeek metro station, killing 32 people. The attacks were also claimed by Daesh and orchestrated by Belgian nationals with links to the Paris attacks.

On 14 July 2016, a 19-tonne lorry was driven into crowds celebrating Bastille Day in Nice, resulting in the deaths of 86 people. The attacker was a Tunisian national with French residency, previously unknown to the security services. It appears that he was radicalised shortly before the attack, and Daesh claimed that it was the work of one of their followers.

On 19 December 2016, a truck was driven into a Berlin Christmas market, killing 12 people. The attacker was a failed Tunisian asylum seeker. Following the attack, Daesh released a video of the attacker pledging allegiance, and purportedly answering their call for 'lone wolf' attacks.

[9] *The information in this box is derived from open source reports.*
[10] *Press conference comments, reported in* The Guardian*, Friday 20 November 2015.*

On 22 March 2017, a car was driven into crowds on Westminster Bridge, after which the attacker attempted to gain entrance to the Houses of Parliament, fatally stabbing a police officer before being shot by armed police. The attack claimed the lives of one police officer and four other people. It is currently assessed that the attacker acted alone.

On 7 April 2017, an attacker drove a lorry into pedestrians in Stockholm, killing five people.

On 22 May 2017, a suicide bomber detonated a device as concert-goers were leaving the Manchester Arena, killing 22 people.

On 3 June 2017, a van was driven into pedestrians on London Bridge. The three occupants of the van, who were all wearing fake suicide belts, then proceeded to use knives to attack people in Borough Market, killing eight people. The three attackers were all shot dead by police.

On 19 June 2017, a van was driven into pedestrians outside a Muslim centre in Finsbury Park, north London, killing one person. The far-right attacker was apparently acting in 'revenge' for recent Islamist terrorist attacks.

On 17 August 2017, a van was driven into pedestrians in Barcelona, killing 14 people. A further person was stabbed to death.

18. Following the Paris attacks in 2015, the then Prime Minister committed to additional investment to combat the threat:

> *The more we learn about what happened in Paris, the more it justifies the full-spectrum approach that we have discussed before in the House. When we are dealing with radicalised European Muslims, linked to ISIL in Syria and inspired by a poisonous narrative of extremism, we need an approach that covers the full range: military power, counter-terrorism expertise, and defeating the poisonous narrative that is the root cause of this evil… we will make a major additional investment in our world-class intelligence agencies.*[11]

19. This was reflected in the 2015 National Security Strategy and Strategic Defence and Security Review (SDSR) which committed an extra £2.6bn over five years to the intelligence and security Agencies to ensure that *"they have the resources and information they need to prevent and disrupt plots against this country at every stage"*.[12] (Although we note that only half of this is additional funding: the remainder is to be found by the Agencies themselves through savings and efficiencies.)

The Threat: Daesh

20. Daesh (also referred to as the Islamic State of Iraq and the Levant/ISIL/ISIS) poses the greatest threat to the UK and its interests around the world. The 'core' Daesh organisation, operating out of Syria and Iraq, has continued to prove its capability to direct large-scale coordinated attacks in Western countries and the Middle East through its

[11] *Prime Minister's statement to the House of Commons, 17 November 2015.*
[12] *National Security Strategy and Strategic Defence and Security Review, 2015.*

'external operations' arm. Daesh propaganda also continues to inspire individuals in Western countries to attempt low-scale attacks in its name.

21. Regionally, the group's territory in Syria and Iraq is under significant military pressure; however, globally it still has a number of affiliated official branches.

Daesh and its affiliates

Daesh in the Arabian peninsula

- Declared as an official Daesh branch in November 2014.
- The group is currently under pressure from local (Saudi) security forces, restricting its ability to conduct attacks in the region.

Daesh in Libya

- Recognised as an official branch by Abu Bakr al-Baghdadi on 13 November 2016.
- Sustained military pressure has restricted the territory held by the group, which has since announced it will continue activity in the region.

Daesh in Yemen

- Recognised as an official branch by Abu Bakr al-Baghdadi on 13 November 2016.
- In the midst of the ongoing civil war, the group continues to prove its capability to conduct large-scale attacks in the region.

Daesh in the Sinai/Egypt

- Recognised as an official branch by Abu Bakr al-Baghdadi on 13 November 2016.
- Daesh in the Sinai has predominantly focused on conducting attacks against Egyptian security forces and State infrastructure in the Sinai peninsula. However, other targets are increasingly being viewed as viable by the group.
- There has been a significant increase in attacks by Daesh-affiliated elements on the Egyptian mainland.

Daesh in the Khorasan Province

- Pledged allegiance to Abu Bakr al-Baghdadi on 10 January 2015.
- The group continues to prove its capability to conduct large-scale attacks in the region; primarily against local security forces and religious interests.

Daesh in West Africa

- Boko Haram pledged allegiance to Daesh and was proclaimed an official branch on 7 March 2015.
- The group has since divided into the Abu Musab al Barnawi-led Daesh-West Africa and the Abubakr Shekau-led Boko Haram.

Daesh in the Caucasus

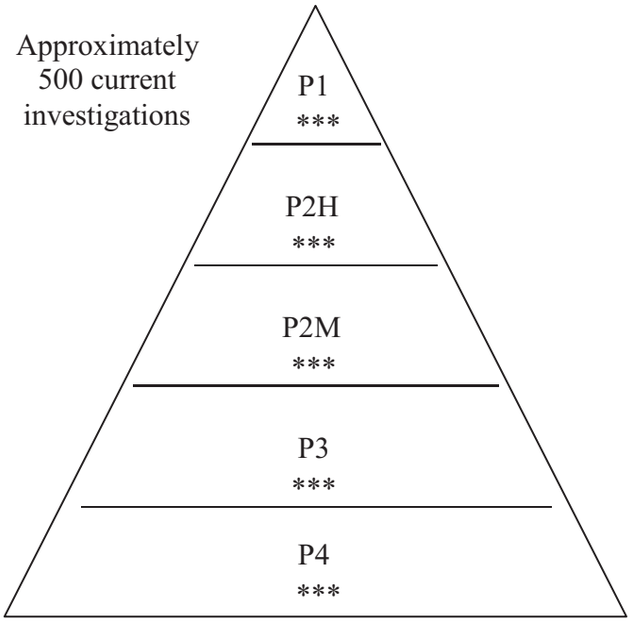
- Proclaimed by Abu Muhammed al-Adnani (former Daesh chief spokesman) on 23 June 2015.
- Operating in the North Caucasus, the group is under continuing pressure from Russian security forces.

The Threat: Scale

22. The scale of the terrorist threat facing the UK is unprecedented in terms of the number of current investigations and the overall number of individuals of interest. As at March 2017, MI5 told us that its investigations have resulted in the disruption of 13 major terrorist attacks since the murder of Fusilier Lee Rigby in May 2013, and that this represents a pace which MI5 has not experienced before.[13]

23. MI5 informed the Committee that, as at April 2017, it was running approximately 500 current investigations into individuals or groups associated with Islamist terrorism.[14] The majority of MI5's investigative effort is allocated against the most high priority of these: *"we… operate according to what we call a weekly grid, which is a top *** investigations week by week that need the most resource ***".*[15]

24. MI5 told us that *"the most striking shift in the composition of CT casework in the last five years was the proportion of what we refer to as high-risk casework"*.[16] Typically, 'high-risk casework' refers to individuals who have received terrorist training or are attempting to procure the means to carry out an attack, but who may not yet have a current attack plan. Previously, these sorts of cases represented a smaller share of MI5's work, with a greater proportion of cases being 'slower burn' in character and requiring less resource-intensive monitoring (for example, relating to radicalisation or fundraising to support terrorism).



P1 : Intelligence of attack planning (comprising P1a and P1b)

P2H : High-risk activity (e.g. terrorist training)

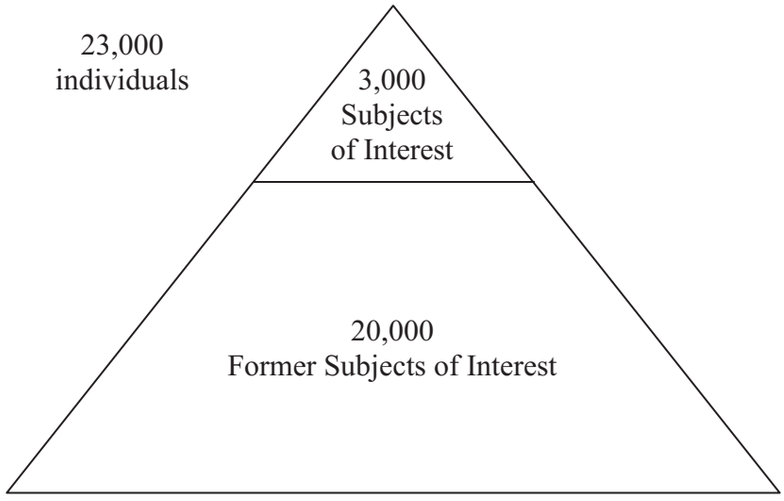
P2M : Medium-risk activity (e.g. terrorist fundraising)

P3 : Investigations into uncorroborated intelligence

P4 : Investigations into individuals at risk of re-engagement with extremist activity

[13] *As of October 2017, this number stands at 20.*
[14] *Written evidence – MI5, 25 September 2017.*
[15] *Oral evidence – MI5, 1 December 2016.*
[16] *Oral evidence – MI5, 1 December 2016.*

25. MI5 also told us that it had around 3,000 Subjects of Interest[17] on its radar, sitting on top of a larger pool of 20,000 individuals who had previously been Subjects of Interest. MI5 has 'tripwires' in place to try to discover if any of these people re-engage in suspicious activity, although it notes that these tripwires will not expose all re-engagement activity.[18]



26. Keeping track of, assessing and applying proportionate investigative resources to such a large number of individuals is an extremely challenging task for the intelligence and security community. MI5 told us:

> *We do sort of lifetime case management, so as soon as we get leads into people, our interest in them starts. We keep our interest in [Subjects of Interest] according to the risk we think they present at any one time. Open-endedly for as long as they are any sort of extremist or threat.* [19]

27. To a certain extent, dealing with volume and ambiguity is 'business as usual' for MI5. Nevertheless, we have been told that the increase in volume is one of the major factors behind the significant extra resources granted to MI5 over the past five years. This has seen its total budget grow from £***m to £***m (a 16% increase) between 2010/11 and 2015/16. MI5 said that the significant extra resources allocated to them were intended to develop its *"capacity to run investigations at a certain scale and provide coverage and the means that we have got to do it"*.[20]

The Threat: Foreign Fighters

28. In December 2016, MI5 told the Committee that, since the start of conflict in Syria in 2011, more than 850 UK-based individuals of national security concern are thought to have travelled to Syria, Iraq and the region. It is believed that around half of those have returned to the UK, more than 300 are thought to remain in Syria, and around 100 have

[17] *A Subject of Interest* "is an individual who is being investigated because they are suspected of being a threat to national security". *In addition to the overall investigation or network being prioritised, every Subject of Interest within that investigation or network is also prioritised.*
[18] *Written evidence – MI5, 4 July 2017.*
[19] *Oral evidence – MI5, 1 December 2016.*
[20] *Oral evidence – MI5, 1 December 2016.*

been killed in fighting in the region.[21] In addition to these UK nationals, it is estimated that approximately 6,000 European fighters have also travelled to fight with Daesh.[22]

29. This requires significant effort from MI5 to identify and prevent individuals from travelling where possible; and when they have travelled, to keep track of their activity overseas, process them on their return and ensure that they do not pose a threat once back in the UK. MI5 described its approach as:

> *For people in the UK wanting to travel [to Syria], in general, we try and stop them because we don't want people developing battlefield experience. ***. So whatever powers there are that we can use that are appropriate in the individual case, we will use.*[23]

30. The authorities use a wide range of methods to prevent individuals from leaving the country including the use of restrictive powers such as TPIMs,[24] the removal of passports and monitoring UK ports of exit.[25] The Office for Security and Counter-Terrorism (OSCT) told us:

> *We have prevented *** people from travelling to Syria and Iraq in 2015. So the numbers going to Syria and Iraq now are down ***.*[26]

31. Nevertheless, it is estimated that more than 300 UK individuals of national security concern remain in the region; when they decide to leave, the UK remains their most natural point of return. It is also worth bearing in mind that other European nationals in Syria and Iraq can be expected to return to their countries of origin at some point and therefore may also pose a threat, both to Europe and the UK.

32. This European dimension means that the effective sharing of information between European security agencies, particularly relating to their respective nationals, is critical. European CT cooperation is discussed in more detail in paragraphs 43–49 and the impact of Brexit on European security is considered more closely in Section 9.

33. As the territory of Daesh is squeezed by military action in Syria and Iraq, the dispersal of this group of foreign fighters becomes a serious concern, raising questions about when and where they will resurface, and what their intentions will be. MI5 told us:

> *I am very concerned about it… A year from now most of them will not be in Syria and Iraq, probably. Who can say how this will unfold?* [27]

In terms of the challenge for the Agencies, MI5 told us:

> *The thing that we do about that is have strong border control informed by comprehensive watch listing of everyone that we know about who has been anywhere near any of these problems. Increasingly identity is backed by biometrics*

---

[21] *Oral evidence – MI5, 1 December 2016.*
[22] *For example, in April 2016, a report by the International Centre for Counter-Terrorism – The Hague estimated that the numbers from EU member states alone could be as high as 4,294. A March 2016 article in* The Telegraph *estimated the numbers for wider Europe were approximately 6,000.*
[23] *Oral evidence – MI5, 1 December 2016.*
[24] *Terrorism Prevention and Investigation Measures.*
[25] *There are other instances where, for example, the family courts have intervened to prevent children from being taken to conflict areas and this has, in turn, disrupted the travel plans of the parent(s).*
[26] *Oral evidence – OSCT, 3 November 2016.*
[27] *Oral evidence – MI5, 1 December 2016.*

and the future path for that for the UK is more and more into biometrics because of… the use of false identity.[28]

34. Where individuals returning to the UK are identified as having been connected to fighting in Syria and Iraq, MI5 explained:

> *We risk assess, in a process with the police, each person as an individual who we identify coming back and we put them into a *** risk structure, which goes from the sort of people… who might be expected to have some sort of terrorist-related intent, right down to [those where] it doesn't look like they want to be involved in this stuff at all. Then the responses to those of course are… 'Pursue-like' response at the top, and then the further down the stack you get, it becomes a 'Prevent' intervention,* ***.[29]

35. A further complication is the number of British – and other European – children growing up inside the so-called 'Caliphate', educated and indoctrinated by Daesh. The reintegration of those who have spent their formative years in such an environment will present a serious challenge for the Government and the Agencies when they return to the UK. The Home Secretary told us:

> *It is absolutely a serious threat. We agree entirely with that. The families coming back will be potentially having children who are going to be vulnerable, who are going to need protecting; but also potentially fighters themselves who could be a danger to society and could radicalise other people. So we are aware of all those different issues… it is something that everybody in Europe is very aware of.*[30]

A. Individuals returning to the UK after having been fighting in Syria and Iraq represent a significant threat to UK security. We recognise the efforts being made to identify, assess and respond to the return of these people to the UK, and urge the Government to ensure that every returnee is fully assessed, that resources are made available such that appropriate monitoring continues on an ongoing basis, and every effort is made to reintegrate children.

[28] *Oral evidence – MI5, 1 December 2016.*
[29] *Oral evidence – MI5, 1 December 2016.*
[30] *Oral evidence – Home Secretary, 2 March 2017.*

The Threat: Directed Versus Encouraged and Inspired Threats

The threat to the UK from Daesh falls into three categories:

- directed threats: where individuals or groups are tasked and supported to carry out attacks against international targets by the 'external operations' arm of Daesh (primarily operating out of Daesh-controlled territory in Syria and Iraq);
- encouraged threats: where individuals or groups in countries such as the UK are encouraged to carry out attacks by Syria-based member(s) of Daesh operating independently from the 'external operations' arm of Daesh. The UK-based individuals or groups may or may not be provided with practical instruction by the Syria-based Daesh member(s); and
- inspired threats: where individuals or groups in countries such as the UK are inspired by Daesh propaganda, predominantly via the internet, to carry out terrorist acts without any direct contact with Daesh itself.

Daesh external operations

36. The primary focus of MI5's International Counter-Terrorism (ICT) work is the prevention of attacks against the UK. It is therefore traditionally associated with a domestic focus. However, in recent years an increasing proportion of MI5's ICT work has been on 'upstream' activity, where 'upstream' refers to action outside the UK such as planning, preparation or direction for an attack in the UK. MI5 told us:

> *We are doing all we can with SIS, GCHQ and international partners to develop intelligence collection on the intent of the people driving terrorist planning from Syria and Iraq… there is part of Daesh which is functionally best described as an external operations department which has a whole bunch of people which pretty much all day every day are plotting terrorism in the West in various countries in various ways, ***.*[31]

37. In practice this means that, although the individuals in question may be outside the UK, MI5 takes the lead, working with GCHQ, SIS and international partners, to investigate and disrupt the threat. Disruption may amount to a criminal justice intervention or, in rare cases in Syria and Iraq, a military intervention.

The inspired threat

38. Daesh also has a significant capability through its extensive media operations to radicalise vulnerable individuals and 'inspire' them to carry out terrorist acts despite not having any direct contact with them. This increases the scale of the challenge facing the security services, both in identifying and disrupting the threat. The Home Secretary told us:

> *There has been a growth in the efforts of Daesh to effectively weaponise people who live here. The onslaught of propaganda against them, to try and make quite often vulnerable young people into extremists is something we have to take action to counter.*[32]

---

[31] *Oral evidence – MI5, 1 December 2016.*
[32] *Oral evidence – Home Secretary, 2 March 2017.*

39. The Director General of OSCT told us that the inspired threat *"is where the growth is and looks like it is going to be going forward"* and as a result we have been told that the Government will be putting more resource into its work under the Prevent strand of CONTEST.[33] We expect the additional resource for Prevent to be confirmed when the revised strategy is published later this year.

Prevent

The Prevent strand of CONTEST covers the Government's counter-radicalisation work to stop people becoming terrorists or supporting terrorism. It seeks to reduce the number of people drawn to violent extremism in Britain by investing in a community-driven approach, working closely with mainstream and moderate groups in the British Muslim community (although the programme addresses all forms of terrorism, including that inspired by far-right extremism). Prevent includes working with industry to remove terrorist material from the internet; supporting civil society groups to deliver effective counter-narrative campaigns; and working with vulnerable people to reduce the risk of them being drawn into extremism, through the Channel programme.

The Channel programme

The Channel programme, which operates under Prevent, was launched in 2007 as a project to identify and support people (across England and Wales) who are at risk of radicalisation. It requires voluntary engagement by the individual referred. Channel interventions can take a variety of forms, including help with youth services, education and housing. The police and other public bodies assist in identifying suitable individuals for referral to the programme. As of March 2014, the Channel project had assessed nearly 4,000 referrals, of which 777 (20%) were deemed vulnerable and received a multi-agency support package to steer them away from radicalisation.

40. Prevent as a brand is, however, not without controversy: many have criticised Prevent as having a significant marginalising effect, in that it places a target on British Muslims and the institutions with which they associate. There is also a sense amongst some parts of the Muslim community that Prevent is about police snooping, and cooperation with the programme can be associated with 'snitching'. Therefore, some argue that the policy is in fact counterproductive.[34] This raises a question as to whether the Government needs to improve engagement with allies within Muslim communities to dispel these myths and improve the reputation of the programme, in order to increase its effectiveness. When we asked the Home Secretary, she told us:

> *I know that Channel, like Prevent, gets a lot of negative publicity. There is a whole industry out there of wanting to knock Channel and Prevent. But… I believe Prevent is successful and we need to increase our efforts.*[35]

The Director General of OSCT added:

> *Prevent is really now about safeguarding vulnerable people… Some of them may fall for the attraction of the charismatic narrative of extremism into terrorism… We had 1,000 people through the Channel programme since 2012.*[36]

---

[33] *Oral evidence – OSCT, 3 November 2016.*
[34] *UN special rapporteur on the right to freedom of assembly, reported in* The Guardian*, 21 April 2016.*
[35] *Oral evidence – Home Secretary, 2 March 2017.*
[36] *Oral evidence – OSCT, 3 November 2016.*

B. The Committee agrees that more must be done to tackle the inspired threat, and welcomes the renewed focus in the latest CONTEST strategy on countering the extremist narrative and helping individuals, particularly those who are most susceptible, to reject radical Islamist ideologies.

Tackling the Threat: Interagency Cooperation

41. Whilst MI5 leads on countering the terrorist threat to the UK, we have noted in previous reports that the Agencies have increasingly been undertaking this work jointly. There are now formal mechanisms and structures, both at operational and leadership levels, to embed this cooperation. SIS considered that, on Counter-Terrorism (CT) work, the three Agencies *"have completely integrated capabilities"*.[37] GCHQ added:

> *Across the CT mission, new ways of working are beginning to show signs of success… We are also seeing much closer integration of [the Agencies'] CT teams… we now have a construct called CT Heads… at Director level all three Agencies are deciding how we are focusing effort on [a] particular operation.*

*** was cited as a good example of the benefits of this joint working:

> *It's been a combination of Agency capabilities to be able [to] achieve ***, that's how we do it and that's exactly what's happened and that's how we've achieved that ***.*[38]

C. The joined-up nature of the Agencies' Counter-Terrorism work is an essential development to ensure that duplication is reduced and to focus the collective effort of the Agencies on the most important issues at a time of increased threat. We are increasingly seeing operational benefits from the approach.

Agency successes

42. Since the murder of Fusilier Lee Rigby in May 2013, as at March 2017 the Agencies have disrupted 13 major attacks against the UK.[39] Given the current scope and scale of the international terrorist threat facing the UK, it is not realistic to assume that all attacks can be prevented and the Agencies have long warned that it is particularly hard to disrupt 'lone-wolf' attacks. It is testament to the outstanding work carried out by the men and women of the Agencies that so many attacks have been thwarted: we do not underestimate the significant pressure on them.

Recent operational successes

The following is a summary of the main disruptions since April 2015. The majority of the activities disrupted were either inspired by Daesh or encouraged by Syria-based Daesh members:

- Operation ***.

  Outcome: The 14-year-old and his girlfriend were arrested for terrorism offences in April 2015. The 14-year-old was sentenced to life imprisonment with a five-year minimum. His girlfriend was sentenced to a one-year intensive referral order.

[37] *Oral evidence – SIS, 17 November 2016.*
[38] *Oral evidence – GCHQ, 19 January 2017.*
[39] *As at October 2017, this figure stood at 20.*

- Operation ***.

  Outcome: Adam Ali, Abdullah Ali and Roman Nikolajevs were arrested in May 2015 and were each sentenced to five years' imprisonment for firearms offences.

- Operation ***: British national Mohammed Rehman (***) and his wife, Sana Ahmed-Khan, aspired to conduct an attack in the UK and were attempting to manufacture explosives.

  Outcome: Rehman and his wife were arrested in May 2015 and have since been given minimum sentences of 27 and 25 years respectively.

- Operation ***: In August 2015, police apprehended UK-based Zahid Hussain in possession of a knife and crowbar. Subsequent police searches recovered chemicals and home-made detonators. ***.

  Outcome: Hussain was detained under the Mental Health Act in 2015 and was sentenced to life with a 15-year minimum sentence.

- Operation ***: Junead Khan devised a plot to attack US military personnel at a UK RAF base. ***.

  Outcome: Khan was arrested in July 2015, and has been sentenced to life imprisonment with a 12-year minimum sentence.

- Operation ***: A radicalised ex-soldier (Gavin Rae) was trying to buy guns to undertake an attack in the UK. ***.

  Outcome: Rae was arrested in November 2015 and was sentenced to 18 years' imprisonment.

- Operation ***. The network, based in Birmingham, had been in contact with Brussels operative Mohammed Abrini.

  Outcome: Mohammad Ali Ahmed, Zakaria Boufassil and Soumeya Boufassil were charged with terrorism offences; Ahmed and Zakaria Boufassil were sentenced to nine and four years respectively in December 2016. ***.

- Operation *** arrest of five Birmingham-based individuals following the recovery of assorted weapons from a vehicle attributed to the group.

  Outcome: Four of the group, including former prisoners Khobaib Hussain, Naweed Mahmood Ali and Mohibur Rahman, were subsequently charged with preparing for acts of terrorism and were sentenced to life imprisonment with a minimum term of between 15 and 20 years.

- Operation *** Haroon Ali Syed was attempting to procure an explosive device and/or firearms for a UK attack after being inspired by Daesh.

  Outcome: Haroon was arrested in September 2016 *** and was sentenced to life imprisonment with a minimum sentence of 15 years.

- Operation ***. In December 2016, Derby-based Eritrean national Munir Hassan Mohammed was arrested.

  Outcome: Mohammed is currently facing four charges under the Terrorism Act, including the preparation of terrorist acts.

Tackling the Threat: Europe

43. The threat from international terrorism transcends national borders, and the recent attacks on the European mainland have clear ramifications for the UK. The attacks have led some European countries to question the capabilities of their security services, particularly regarding their ability to work collaboratively.[40] For example, there are numerous reports of the perpetrators of the attacks in Paris in November 2015 being known to the French and Belgian intelligence services and police, and yet the authorities failed to piece together all the available information or establish the cross-border links between what were known extremists. Stark examples of these problems relate to the escape from Paris of Salah Abdeslam and two others in the aftermath of the attack. Crucial evidence from the vicinity of the Bataclan attack (a car rental agreement in Abdeslam's name) was overlooked by the police for a number of hours, meaning his potential involvement had not been alerted to border police. Crucially, when police at the border did check his details in the Schengen Information System they found only historic criminal records, with no reference to his jihadist links, and he was allowed to continue his journey to Brussels.

44. In July 2016, a French parliamentary commission called for an overhaul of the country's intelligence services, after an inquiry into the Paris atrocities highlighted serious shortcomings in the run-up to the attacks. Georges Fenech, head of the Commission, stated: *"Our country was not ready; now we must get ready."*[41]

45. It appears that the capabilities of some countries had historically been overestimated. ***:

***.[42]

This question of capability has placed greater emphasis on the UK's contribution to the European intelligence community. MI5 told us: *"***"*.[43] MI5 deployed liaison officers to other countries in the wake of attacks, both to provide support to the national responses, but also to understand better the nature of the threat to the UK. GCHQ also told us that it is investing greater resource in building its relationship with ***, and more broadly that its work has identified a number of previously unknown threats in Europe, ***.[44]

Counter-Terrorism Group

46. The Counter-Terrorism Group (CTG) is an avowed group of 30 European domestic intelligence services working outside EU structures, which meets to *"discuss areas of mutual interest, share operational experiences, and exchange information"*.[45] It was established in 2001, in response to the 9/11 terrorist attacks.

---

[40] *For example, writing in the German newspaper the* Frankfurter Allgemeine Zeitung *on 3 January 2017 (in the wake of the December 2016 attack on a Christmas market in Berlin) the German Minister of the Interior, Thomas de Maizière, noted:* "We have no federal responsibility for national disasters. The responsibilities for combating international terrorism are fragmented. The federal police is limited in its effect on railway stations, airports and border security… the federal government needs to have control over all security agencies… we need uniform rules and better coordination, for example regarding the control of threats."

[41] *Press conference comments, reported in* The Guardian*, 5 July 2016.*

[42] *Oral evidence – OSCT, 3 November 2016.*

[43] *Oral evidence – MI5, 1 December 2016.*

[44] *Written evidence – GCHQ, 31 January 2017.*

[45] *Written evidence – MI5, 30 August 2016.*

47. MI5 told us that there are currently *"unprecedented levels of cooperation with 5 EYES, CTG and a [tri-Agency] approach"*[46] and that:

> *[The] CTG provides huge added value in the way MI5 conducts business with our European colleagues. It is a vital tool for exporting the UK view of the threat and galvanising action… bringing our understanding together has inevitably made our combined effort stronger… multilateral intelligence sharing in the wake of the attacks in Paris and Brussels helped identify leads*.[47]

48. MI5 has assured us that the UK's decision to leave the European Union will not adversely impact on its membership of, and participation in, the CTG.[48] However, the presidency of the CTG rotates in accordance with the presidency of the Council of the EU. We asked MI5 whether it would continue to have the opportunity to take on the presidency of the CTG once the UK has left the EU, and it replied as follows:

> *The UK had been due to take on both [Council of the EU and CTG] Presidencies in July this year. However, following the Brexit vote, the Prime Minister decided that the UK should not take on the EU Presidency. This then devolved to the next Member State in the succession – Estonia. With agreement from KAPO (the Estonian Internal Security Service) – indeed with consensus across the CTG – MI5 and KAPO will hold the CTG Presidency jointly.*[49]

MI5 did not comment on whether it is likely to have the opportunity to take on the presidency of the CTG in what would have been the next iteration of the UK's presidency.

49. The broader impact of Brexit on the ability of the UK security services to continue to work with European partners is considered in more detail in Section 9.

Lessons Learned: Recent Attacks

50. The recent events in Europe have demonstrated the growing range of techniques being used to carry out terrorist attacks, including the use of vehicles and automatic weapons in addition to more traditional attacks utilising explosives.

Marauding firearms attacks

51. The Committee has been told that the terrorist attacks in Paris in November 2015 directly contributed to the decision to increase the UK's armed response capability in terms of the number, capability and deployability of firearms officers and their ability to respond to multiple attacks. MI5 told us: *"the Paris attacks happened virtually in the same week as the Chancellor was making decisions about the Spending Review last year and became a big… factor in it."*[50] The Home Secretary informed us that responding to marauding firearms attacks has been an area of significant focus in the national programme of CT exercises coordinated by OSCT.[51]

---

[46] *Written evidence – MI5, 28 October 2016.*
[47] *Written evidence – MI5, 30 August 2016.*
[48] *Written evidence – MI5, 30 August 2016.*
[49] *Written evidence – MI5, 21 April 2017.*
[50] *Oral evidence – MI5, 1 December 2016.*
[51] *Oral evidence – Home Secretary, 2 March 2017.*

52. However, MI5 emphasised that whilst the increase in the response capacity was welcome, its primary focus was to prevent events like this from happening in the first place:

> *The UK has a really strong response now in capacity which is, you know, mobile and good numbers for multiple incidents so there is a 'Prepare' bit if this gets past, but for MI5, we look at these things, you know, and think the best answer is this doesn't happen in the first place. So [there] is another drive to jack up the intelligence coverage.*[52]

53. MI5 and OSCT both emphasised that the relative difficulty of obtaining firearms in the UK (compared with on the Continent) is a *"strategic advantage"* and noted that significant work is continuing to ensure that this remains the case.[53] OSCT told us:

> *On firearms… there is increasing collaboration between the NCA [National Crime Agency] and the CT police in those areas where one of our great strategic advantages is it is hard to get hold of firearms in the UK… It is still relatively hard, certainly compared to the continent, to get hold of weapons. There is a significant amount of work to make sure that stays that way.*[54]

Vehicle attacks

54. The appalling attack in London on 22 March 2017, where the attacker killed and injured pedestrians on Westminster Bridge before fatally stabbing a police officer, was an attack which involved the use of a vehicle as a weapon of terror. Such attacks require no specialist equipment and can cause significant harm in a short period of time. The Westminster attack lasted just 82 seconds, but it killed five people and injured 50. Even with a rapid police response, such attacks are extremely difficult to prevent. Nevertheless, there are always lessons to be learned from such tragic events, and once the immediate operational activity has subsided, we will be considering this in more detail.

55. Following the lorry attacks in Nice and Berlin, we requested information on the Government's response, and work to protect against such attacks in the UK. The Home Secretary told us that *"we will always make sure that where something has happened in an incident which creates a new route, that we learn from it and find a way of addressing it"*.[55] The day after the lorry attack in Nice, the police held an extraordinary meeting of the Security Review Committee. The results of this included:

- a review of all upcoming events to ensure existing security plans remain proportionate and appropriate;
- adjusting the focus of police protective security patrols to give greater priority to crowded places; and
- further consideration of where more could be done to mitigate against the vulnerabilities around HGVs being used in such attacks in the UK.[56]

---

[52] *Oral evidence – MI5, 1 December 2016.*
[53] *Oral evidence – OSCT, 17 November 2016; oral evidence – MI5, 1 December 2016.*
[54] *Oral evidence – OSCT, 17 November 2016.*
[55] *Oral evidence – Home Secretary, 2 March 2017.*
[56] *Written evidence – OSCT, December 2016.*

The Centre for the Protection of National Infrastructure

The Centre for the Protection of National Infrastructure (CPNI) is accountable to MI5. It gives advice on protective security to owners of critical national infrastructure in government and the private sector and, as national technical authority for physical and personnel security, develops a range of measures suitable for use at other sites such as crowded public places. CPNI advice aims to reduce the vulnerability of key physical, personnel and information assets to attack, by terrorists or Hostile State Activity. It works closely with the National Cyber Security Centre in relation to protective security in the cyber arena.

56. In addition, CPNI helped to devise and test *"a number of temporary and permanent measures designed to stop a truck such as the one used in the Nice attack",*[57] and the Home Secretary told us that the Government has been working with the UK Road Haulage Association to help ensure that its members have the appropriate security measures in place for their vehicles and staff.

57. Areas around UK Government buildings and other high-risk sites are protected by a range of overt and covert measures to reduce the likelihood and impact of hostile vehicle attacks. However, many other areas remain unprotected and are vulnerable to attacks. In addition to some public spaces, many of the locations likely to be targeted in this type of attack are privately owned. The Government's work in this area involves working closely with the private sector to ensure 'hostile vehicle mitigation' considerations are factored in at the design stage of new developments, and providing advice on how existing sites can be made less vulnerable. The Home Secretary emphasised the importance of this approach, noting that *"we really lean into the private sector to make sure they can have the right tools and the right training, where necessary"*.[58] The following box provides an overview of the Government's existing work to protect against vehicle attacks.

Case study – UK protection against vehicle attacks

In 2012, OSCT worked with the police, the Joint Terrorism Analysis Centre (JTAC) and the CPNI to seek to identify those crowded places (tourist attractions, stadiums, shopping centres, etc.) in the UK most likely to attract a terrorist attack. Since then, all those places which have been identified as priorities have been offered bespoke protective security advice and guidance through the national network of approximately 170 police Counter-Terrorism Security Advisers (CTSAs).[59]

CTSAs work in partnership with the sites to develop plans to improve site protective security and preparedness against a range of attack methodologies, including vehicle-based attacks. Advice to sites is provided free of charge but implementation of measures is on a 'user pays' principle. The Committee has been told that although there is no legislation to compel sites to engage with CTSAs or implement particular security measures, over 98% of these priority sites have engaged with the process.[60]

---

[57] *Written evidence – MI5, 29 July 2016.*
[58] *Oral evidence – Home Secretary, 2 March 2017.*
[59] *The managers of all crowded places have access to information and advice through the National Counter-Terrorism Security Office and CPNI websites.*
[60] *Written evidence – OSCT, December 2016.*

The policing of temporary events such as festivals, demonstrations and occasional sporting events is a feature of routine policing activity. Local forces identify and review security measures for local events, deploying physical protection and guarding as appropriate to the level of threat and vulnerability. These security measures are reviewed on a regular basis as a matter of routine or in response to a terrorist incident such as the Nice attack.[61,62]

Lessons Learned: Terrorism Prevention and Investigation Measures

58. In January 2012, the system of Control Orders was replaced by the TPIMs regime. TPIMs place restrictions on individuals who are assessed to pose a terrorist threat, but who either cannot be prosecuted, for example because of insufficient disclosable evidence, or who have been prosecuted, released and assessed to continue to pose a threat. However, this Committee has previously expressed concern about the increase in overall risk when compared with Control Orders, since TPIMs lacked the power to relocate individuals away from extremist networks or other radicalising influences.[63] In March 2014, the Government's Independent Reviewer of Terrorism Legislation, David Anderson QC, also noted that the relocation element of Control Orders (absent from the new TPIMs regime) offered significant advantages from a national security point of view.[64] Between February 2013 and May 2016, the number of individuals subject to TPIMs fluctuated between one and three (throughout which time the terrorist threat remained SEVERE), leading to questions about how useful TPIMs actually were to the security services over this period.

59. We were therefore encouraged to see that the Counter-Terrorism and Security Act 2015 made a number of amendments to TPIMs. The most notable of these was the restoration of the 'relocation power', previously associated with Control Orders, under which TPIM subjects can be required to live up to 200 miles from their home and local associates. This has apparently led to an increase in the number of TPIMs being issued: in March 2017, this had increased to seven (the highest level in two and a half years).[65] We questioned OSCT on the link between the reintroduction of the relocation powers and the increase in their practical use and they confirmed that *"In our assessment, the reintroduction of relocation has made the TPIM regime more effective"*.[66]

D. We welcome the recognition by the Government of the concerns of this Committee and the Independent Reviewer of Terrorism Legislation around the risks associated with the TPIM regime, and the subsequent reintroduction of the relocation element to provide a more effective mechanism for the security services and the police to manage the threat posed in these areas.

---

[61] *Written evidence – OSCT, December 2016.*
[62] *The police also have access to the National Barrier Asset, which is made up of a range of temporary hostile vehicle mitigation equipment, security fences and gates that enable temporary physical protection of sites. OSCT told us that the National Barrier Asset is particularly useful in deterring vehicle-based attacks.*
[63] Intelligence and Security Committee Annual Report 2011–2012*, Cm 8403, July 2012.*
[64] Second Report on the Operation of TPIMs*, March 2014.*
[65] *Oral evidence – Home Secretary, 2 March 2017.*
[66] *Written evidence – OSCT, 5 December 2016.*

Managing convicted terrorism offenders

60. Continuing to monitor individuals convicted of terrorist offences whilst in prison, and after their release, falls to the police and MI5. MI5 told us that in 2016 there were 36 people released who were in prison under terrorist offences,[67] and that:

> *The prison population… is something approaching 200. It [the number released] is going to be more than that in the next two years… it will keep being a strand of our work that we will have to manage these numbers.*[68]

61. The Home Secretary told us that she recognised that the increasing number of individuals in prison for terrorism-related offences, and those nearing the end of their sentences, is a significant new threat area which places further strain on the resources of the security services:

> *We have 180 Terrorism Act offenders now in prisons; that is up 70 per cent in the last three years. So we need to make sure that we are managing this end to end and need to invest across that chain.*[69]

Lessons Learned: Review of CONTEST

CONTEST

- The Government developed its first comprehensive counter-terrorism strategy, known as CONTEST, in 2003. Following the 7/7 terrorist attacks in London, the Government published the strategy in July 2006. A 'refresh' of CONTEST was published in March 2009, and the current version was published in July 2011.
- The CONTEST strategy focuses on four key elements: Pursue, Prevent, Protect and Prepare (colloquially known as the 'Four Ps'):
    - Pursue: the investigation and disruption of terrorist attacks;
    - Prevent: the work to stop people becoming terrorists or supporting terrorism;
    - Protect: improving our protective security to stop a terrorist attack; and
    - Prepare: working to minimise the impact of an attack, and to recover as quickly as possible.

62. We have been told that the Government will soon be relaunching an updated CONTEST strategy. At the time of writing, we have not been provided with the updated document; however, we understand that there have been a number of significant changes. The Director General of OSCT told us:

> *We still feel that the Four Ps work but they are much less linear now, they used to be that you could draw a nice graph of the Four Ps, all… elegantly… conducting their business but the way the threat has emerged to be much more variegated in how it conducts attacks and its use of the internet to break down the barriers between*

[67] *Written evidence – MI5, 4 July 2017.*
[68] *Oral evidence – MI5, 1 December 2016.*
[69] *Oral evidence – Home Secretary, 2 March 2017.*

internal and domestic, means that actually where Pursue ends and Prevent begins, these lines are blurring and that will change the way we approach it.[70]

63. OSCT told the Committee that the review had been thorough and included considering, and learning from, the deficiencies in the previous iterations:

> *JTAC provided seven scenarios of what the threat might look like going forward and we matched, through 40-odd workshops, how our [selection] of capabilities looked against those scenarios, involving… hundreds of people across the community.*
>
> *We did fail to look ahead far enough and we did fail to see the rise of ISIL, and this does, okay, come not that hot off the foot of also failing to see the rise of Al-Qaeda, many years ago. So the community is extremely good at dealing with the present threat but is not really culturally configured very well to look further ahead and therefore, you know, we need to change that, because, as I mentioned, CONTEST is around countering terrorism, it is not just about countering the terrorists of today.*[71]

64. The Home Secretary said: *"there are a number of key elements where we have acknowledged that there are changes in the threat and where we need to take action and therefore reprioritise"*. She told the Committee that the key themes of the new CONTEST strategy included:

- a greater focus on Prevent, to address *"the efforts of Daesh to effectively weaponise people who live here"*;
- managing the return of foreign fighters from Syria and the region;
- further effort on de-radicalising terrorists in prison, and monitoring them effectively on their release;
- improving the UK's border security; and
- working more closely with international partners and the private sector on counter-terrorism.[72]

[70] *Oral evidence – OSCT, 17 November 2016.*
[71] *Oral evidence – OSCT, 17 November 2016.*
[72] *Oral evidence – Home Secretary, 2 March 2017.*

SECTION 4: NORTHERN IRELAND-RELATED TERRORISM

65. MI5 told the Committee that Northern Ireland represents the *"most concentrated area of terrorist activity probably anywhere in Europe",* with terrorist activity disrupted on a weekly basis.[73]

66. The threat level in Northern Ireland remains SEVERE, meaning an attack is highly likely. The threat to Great Britain from Northern Ireland-related terrorism, which is assessed separately to the threat in Northern Ireland, was raised to SUBSTANTIAL in May 2016. This means an attack in Great Britain is a strong possibility.

67. Whilst loyalist groups continue to exist, MI5 assesses that the national security threat comes overwhelmingly from dissident republicans. Dissident republicans conducted 16 terrorist attacks on national security targets in 2015/16. According to MI5, the 'new IRA' is the dominant threat and has continued to extend its capability and ambition although the Continuity IRA and Óglaigh na hÉireann remain active.

68. The 'new IRA' murdered prison officer Adrian Ismay in Belfast in March 2016 by placing an IED under his vehicle. Mr Ismay was the first security force fatality in Northern Ireland since the murder of prison officer David Black in 2012. In February 2017, the 'new IRA' claimed responsibility for an IED under the vehicle of a police officer; the device did not function as intended but detonated whilst under examination by a military bomb disposal team (with no casualties).

69. MI5 assesses that the threat from dissident republicans remains resilient, despite significant security force pressure from MI5 and the police. In 2015/16, there were more than 250 disruptions carried out against dissident republican groups by MI5, the police and other partners, including significant seizures of munitions and explosives, arrests and charging of key personnel. MI5 explained that its current approach severely constrains the terrorists' ability to conduct successful attacks: *"there are many many many attempts, very few are translated into actual acts of terrorism because of what we and the police are doing".*[74] However, MI5 assesses that the ambitions of the 'new IRA' are undimmed. The leadership has been strengthened by prison releases and the morale of the membership was likely to have been buoyed by the murder of Adrian Ismay. Despite the disruptions and seizures in the last 12 months, MI5 believes that the 'new IRA' retains access to terrorist material that includes firearms, ammunition and explosives, and that further potentially lethal attacks are therefore highly likely.

70. MI5 also told us that there have been a number of 'disappointing' criminal justice outcomes recently – including sentences that were shorter than the authorities had expected, and a case against a senior 'new IRA' member that was abandoned due to concerns over the disclosure of sensitive material.

[73] *Oral evidence – MI5, 1 December 2016.*
[74] *Oral evidence – MI5, 1 December 2016.*

71. As of 31 March 2016, *** Northern Ireland-related terrorism accounted for around 18% of MI5's operational and investigative resources. We questioned MI5 as to whether the balance of resource was correct, given that 64% of its effort is focused on international counter-terrorism. MI5 told us:

> *We are in sustain mode as far as counter-terrorism and Northern Ireland goes because we are eating into the problem and if we stick at it we will keep driving it down…*
>
> *I wouldn't want the Committee to feel that if we pressed the pedal much harder in resource terms, it would be achievable to get down to zero violence or negligible levels. It cannot happen that way and I think there would be diminishing returns if one were to attempt that.*[75]

E. We commend the efforts of MI5 and the Police Service of Northern Ireland in limiting the number of Northern Ireland-related terrorism attacks. However, at a time when the threat level has been raised, it is important that they are able to maintain the current pressure on the 'new IRA', in particular.

[75] *Oral evidence – MI5, 1 December 2016.*

SECTION 5: CYBER SECURITY

The Threat: Scope

72. The current cyber threat to the UK is diverse, ranging from state actors such as Russia, China and Iran, to organised crime groups and terrorist organisations, to individual criminals. All sectors of society are at risk, from government networks, to companies, to individuals. GCHQ told the Committee that two years ago it had predicted *"the tidal wave of cyber attacks to rise internationally and in the UK, and… a major attack in the next year".*[76]

State actors generally possess the most sophisticated cyber capabilities, which are most often employed against the state or large companies. Their objectives typically include commercial gain (e.g. stealing commercial secrets), geopolitical gain (e.g. interfering in another country's elections or causing instability) and more traditional espionage (e.g. stealing 'state secrets'). The practical use of the advanced capabilities possessed by state actors may often be tempered by diplomatic or geopolitical considerations.

Organised criminals represent the next most sophisticated threat group, generally targeting individuals or organisations for financial gain. This may involve the theft of bank details and personal information, or holding systems 'for ransom' until payment is made.[77]

Terrorist groups are prepared to use cyber techniques; however, there is no evidence of them successfully carrying out cyber action intended to cause direct harm, and most commentators suggest they lack the requisite capabilities. The use of the internet by terrorist groups therefore mainly relates to spreading propaganda.

'Real-world' impact

73. Many of the current cyber threats facing the UK involve damage to the economy, individual prosperity or privacy. However, increasingly there is a risk of physical damage in the 'real world'. The number of devices, processes and functions connected to the internet – ranging from parts of the Critical National Infrastructure to wifi-enabled domestic appliances – has grown exponentially in recent years. The Internet of Things (IoT) is a term used to refer to physical devices (including home appliances, vehicles and buildings) embedded with electronics, software, sensors and network connectivity that enables them to collect and exchange data, and that connectivity makes them vulnerable to cyber attack with potential for direct 'real-world' impact.

74. Developing secure systems is an expensive and time-consuming business, and historically the devices which make up the IoT have not been designed with cyber security in mind. This has resulted in vast, often insecure, networks, creating easy targets for hackers. In October 2016, a US internet routing company (Dyn) was targeted by a massive

[76] *Oral evidence – GCHQ, 19 January 2017.*

[77] *There can be some overlap between state actors and organised criminals, as some foreign intelligence services (***) are known to use criminal groups to augment their cyber capabilities and obscure state involvement in such activities.*

DDoS attack.[78] This involved networked household devices around the world, particularly webcams and digital video recorders, being infected with malware and used to direct huge amounts of traffic towards the company's servers, bringing down internet access to numerous popular sites for many users.[79] Commentators have estimated that this was the most powerful DDoS attack on record, facilitated by more than 100,000 infected IoT devices (producing 1.2Tbps of traffic – roughly twice the previous record).[80]

75. A number of 'secure' operating systems for the IoT are currently under development (by technology companies such as Google, ARM and others). This will provide more straightforward options for manufacturers to build the electronics of future systems based on a more secure platform – if they choose to do so. However, until consumers or regulators demand better security, many manufacturers are likely to side-line cyber security considerations, given their potential impact on time to market and, therefore, profits. GCHQ told us that: *"people are producing very cheap devices where they don't want to spend time and money on security"*.[81]

F. Government must work closely with industry internationally to promote the use of modern and secure operating systems in all smart devices connected to the internet. One option could be an accreditation standard for 'approved' Internet of Things (IoT) devices to help guide consumers.

Recent cyber attacks

(i) Information and data breaches

- TalkTalk – the personal details of nearly 157,000 customers were stolen. This was found to be an unsophisticated attack carried out by a British teenager, demonstrating the low barriers to entry for relatively high-impact attacks. In this case it was allowed by *"TalkTalk's failure to implement the most basic cyber security measures"*.[82]
- US Office of Personnel Management – an attack resulted in records of 21.5 million federal employees being stolen. This is likely to have included the theft of highly sensitive security clearance-related background information. The hack has been widely reported to have originated from China, although US officials have not confirmed whether they believe it to have been state sponsored.
- Sony Pictures – North Korean hackers compromised the systems of Sony Pictures prior to the release of a film depicting their leader in a demeaning light. This resulted in the film being pulled from cinemas, although it was subsequently re-released.
- US Democratic National Committee – the hacking of email accounts belonging to the Democratic National Committee and senior Democratic officials. US agencies have publicly stated that they believe the Russian State was behind the attack, and that this was part of a wider campaign to influence the outcome of the US presidential election.[83]

[78] *Distributed Denial of Service attack.*
[79] USA Today*, 21 October 2016; oral evidence – GCHQ, 19 January 2017.*
[80] Lessons from the Dyn DDoS Attack*, Schneier on Security (www.schneier.com), 8 November 2016.*
[81] *Oral evidence – GCHQ, 19 January 2017.*
[82] *Information Commissioner, press statement, 5 October 2016.*
[83] *US Intelligence Community Assessment,* Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 6 January 2017.*

(ii) Disruptive attacks/'real-world' impact

- A series of attacks against Ukrainian electrical power distribution companies in December 2015 caused widespread blackouts. US investigators accused Russian-based hackers.
- A 'hacktivist' group with ties to Syria compromised the systems of an (as yet unnamed) water company which regulate the chemicals added to the water supply (reported in the *Verizon Security Solutions March 2016* security breach report).
- A group widely thought to be associated with the Russian State crippled a French TV broadcaster's network (TV5Monde) whilst masquerading as 'ISIL hackers'.

The Cyber Threat: Terrorists

76. The Committee has previously been told that whilst terrorist groups have the intent to cause harm through cyber attacks there is no evidence of them successfully doing so, and most commentators suggest they lack the requisite capabilities. Indeed, their use of the internet is primarily as a media and communications tool. In 2015, the then Chancellor, George Osborne, noted in a speech at GCHQ:

> *ISIL are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too. They have not been able to use it to kill people yet by attacking our infrastructure through cyber attack. They do not yet have that capability. But we know they want it and they are doing their best to build it.*[84]

This assessment does not appear to have changed. In January 2017, GCHQ told us that it still believes that terrorists' capability to conduct cyber attacks is currently *"***... but that's not to say that one day the intent and the capability won't meet, because they usually do"*.[85]

77. We note that one way in which terrorist groups might attain that capability is by 'buying in' expertise from organised criminal groups. GCHQ told us that *"the thing that could shorten the timescales is the development by serious and organised criminals of capability they would be prepared to sell to a terrorist organisation and that's one of the things that we're... keeping a very close eye on"*.[86] We consider organised crime groups later in this section.

The Cyber Threat: State Actors

78. State actors are highly capable of carrying out advanced cyber attacks; however, their use of these methods has historically been restricted by the diplomatic and geopolitical consequences that would follow should the activity be uncovered. Recent Russian cyber activity appears to indicate that this may no longer be the case.

79. In October 2016, in the midst of the US presidential election campaigns, emails belonging to the Democratic National Committee and John Podesta (Hillary Clinton's top aide) were gradually released via WikiLeaks – the content of which placed significant

[84] *George Osborne, speech at GCHQ, 17 November 2015.*
[85] *Oral evidence – GCHQ, 19 January 2017.*
[86] *Oral evidence – GCHQ, 19 January 2017.*

pressure on the Clinton campaign. Media reports began to surface regarding outside interference in the election and, although many suspected Russian involvement, this was not confirmed until 7 January 2017 when the US intelligence community published an official assessment. That report said:

> *We… assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavourably to him.*
>
> *We assess with high confidence that Russian military intelligence used the Guccifer 2.0 persona and DCLeaks.com to release US victim data obtained in cyber operations publicly and in exclusive to media outlets and relayed material to WikiLeaks.*
>
> *… these activities demonstrated a significant escalation in the directness, level of activity, and scope of effort compared to previous operations.*[87]

80. Such escalation clearly indicated that Russia was no longer concerned about its activities remaining covert, and that it was adopting a more brazen approach to its cyber activities. GCHQ told us:

> ***.[88]

MI5 told us: *"***".*[89] (The broader threat to the UK from state actors, including Russia, China, North Korea and Iran, is discussed in more detail in Section 8.)

G. The combination of the high capability of state actors with an increasingly brazen approach places an ever greater importance on ensuring the security of systems in the UK which control the Critical National Infrastructure. Detecting and countering high-end cyber activity must remain a top priority for the Government.

Security of the UK's political system

81. The UK's political system is a potential target for cyber attacks by hostile foreign states and terrorist groups. Such attacks could include hacking into parliamentary or private computer networks and obtaining communications and data belonging to political figures, or obtaining the sensitive data on the electorate which is held by political parties. It could also potentially include planting fake information on legitimate political and current affairs websites, or otherwise interfering with the online presence of political parties and institutions. GCHQ explained how it is already alert to the risks surrounding the integrity of data:

> ***.[90]

82. This sort of attack could have various objectives, including:

- generally undermining the integrity of the UK's political processes, with a view to weakening the UK Government in the eyes of both the British population and the wider world;

---

[87] *US Intelligence Community Assessment,* Assessing Russian Activities and Intentions in Recent US Elections*, 7 January 2017.*
[88] *Oral evidence – GCHQ, 19 January 2017.*
[89] *Oral evidence – MI5, 1 December 2016.*
[90] *Oral evidence – GCHQ, 19 January 2017.*

- subverting a specific election or referendum by undermining or supporting particular campaigns, with a countervailing benefit to the hostile actor's preferred side;
- poisoning public discourse about a sensitive political issue in a manner that suits the hostile state's foreign policy aims; or
- in the case of political parties' sensitive data on the electorate, obtaining the political predilections and other characteristics of a large proportion of the UK population, thereby identifying people who might be open to subversion or political extremism in the hostile actor's interests.

83. Following the revelations about Russian interference in the 2016 US presidential election, the Committee sought assurance from the Government that adequate consideration was being given to protecting the UK's political system from cyber attack. GCHQ told us that *"protecting the UK's political system from hostile cyber activity is a major operational priority for the National Cyber Security Centre"*,[91] and that work to counter it includes a range of measures designed to address the threats identified in the UK and elsewhere. These include:

- *Tracking the major known perpetrators of these types of attacks and reporting detected incidents to those affected …;*
- *Ensuring that individuals whose participation in political activity puts them in the public eye, have easy access to best practice advice on their private communications security;*
- *Working with media, think tanks and other organisations to help defend against activity to undermine open and free discourse and debate through targeted attacks, disruption and the generation of propaganda (such as those we saw in France in 2015 and have seen against think tanks);*
- *Making it easier for organisations that hold a significant amount of personal data, including political parties and local constituency offices, to meet their obligations to protect it.*[92]

We were also told, in February 2017, that the Minister for the Cabinet Office has *"instituted an interdepartmental programme of work to put measures in place to assure the integrity of the UK's democratic processes against hostile state influence"*.[93]

84. On the specific subject of the security of parliamentarians' communications and data, GCHQ said:

> *We monitor the executive, we monitor Government departments, we do not monitor Parliamentary networks. We have a good relationship with the Parliamentary security team and we have given advice to individual parliamentarians. On your first day, I think, in this Parliament we sent everybody leaflets on what to do and who to go to for advice. So we can [do] all of that but it is not part of our remit in the same way.*[94]

---

[91] *Written evidence – GCHQ, 16 February 2017.*
[92] *Written evidence – GCHQ, 16 February 2017.*
[93] *Written evidence – GCHQ, 16 February 2017.*
[94] *Oral evidence – GCHQ, 19 January 2017.*

However, GCHQ has made it clear that there will always be an element of personal responsibility needed:

> *You could have made the [Democratic National Committee] the best defended network in the world and it would still have got John Podesta's Gmail. So it still would have a trove of embarrassing data because [he] hadn't switched on two-factor [authentication]… It makes it much harder to attack a personal email account and it wasn't switched on.*[95]

85. Regarding the protective security of political parties' datasets on the electorate, GCHQ initially made clear that it does not have a direct mandate to cover this:

> *I think ultimately it's a choice for parties as to how much they want us involved. I mean, post-Snowden, if I had rocked up to political parties a year ago and said would you like us to come into your databases just to check things are okay, you could imagine what people would have said. But there's a lot of paranoia, and we've never been asked by a political party, but the advice is all there and we can absolutely do it.*[96]

In March 2017, however, after encouragement from this Committee, the head of the National Cyber Security Centre wrote to the leaders of the UK's major political parties[97] directly offering its assistance in protecting their data and networks.

H. We welcome GCHQ's offers of assistance and advice to political parties and parliamentarians to improve the security of their networks and data, and encourage all those concerned to accept.

The Cyber Threat: Organised Criminals

86. Cyber crime remains a significant issue – whilst previously this was the preserve of a small cadre of niche experts, today 'cyber attack services' are being bought and sold as commodities via anonymised web services. We have been told that some criminal organisations are using management systems and business methodologies to assess the profitability of different lines of attack, so that they can ensure they prioritise their efforts in the most profitable areas.[98] GCHQ told us:

> *The criminal dimension takes pretty much every form you can think of. It can take [take the form of] small groups in the UK [and allied countries], not terribly sophisticated, where law enforcement can act with relative ease. But there are some extremely sophisticated groups operating in countries where we have no law enforcement reach, and *** is a particularly difficult example, where the operations are very sophisticated.* [99]

---

[95] *Oral evidence – GCHQ, 19 January 2017; two-factor authentication refers to a system where a second form of security (often a security token or a verified mobile phone) is needed in addition to a user's normal password.*
[96] *Oral evidence – GCHQ, 19 January 2017.*
[97] *Defined as those with two or more MPs in the House of Commons.*
[98] *Oral evidence – GCHQ, 19 January 2017.*
[99] *Oral evidence – GCHQ, 19 January 2017.*

Criminal cyber attacks: *

In 2015, the UK was subject to a major criminal cyber attack using 'Dridex' malware, aimed at stealing users' personal information (often bank details). ***:

> **** it was [a] sustained attack on I think half a million British people, [involving a variety of sources of data including some Government data] and that sort of thing, ***.*[100]

The Government Response: Strategy

87. This Committee has closely examined the Government's Cyber Security Strategy over the past decade. In its 2008–2009 Annual Report, the Committee raised concerns about the potential threat posed to the UK Government, Critical National Infrastructure and commercial companies from electronic attack and recommended that the UK accord cyber security a higher priority.[101] Since 2009, when the first Cyber Security Strategy was launched, the Committee has continued to follow developments closely. In July 2012, we said:

> *Twenty months into the National Cyber Security Programme, there appears to have been some progress on developing cyber capabilities. However, cyber security is a fast-paced field and delays in developing our capabilities give our enemies the advantage. We are therefore concerned that much of the work to protect UK interests in cyberspace is still in an early stage.*[102]

The following year we noted:

> *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.*[103]

88. In the five years between 2011 and 2016, the Government allocated £860m to the National Cyber Security Programme, which was distributed between various Government organisations. For the five years from 2016 to 2021, the Government has – in recognition of the threat – significantly increased funding and allocated £1.9bn for the new National Cyber Security Strategy. This new strategy (published in November 2016) is centred on the following objectives:

> *DEFEND: We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses, and the public sector have the knowledge and ability to defend themselves.*
>
> *DETER: The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing*

[100] *Oral evidence – GCHQ, 19 January 2017.*
[101] *ISC Annual Report 2008–2009, Cm 7807.*
[102] *ISC Annual Report 2011–2012, Cm 8403.*
[103] *ISC Annual Report 2012–2013, HC 547.*

and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.

DEVELOP: We have an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. We have [a] self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis will enable the UK to meet and overcome future threats and challenges.[104]

GCHQ's implementation of the strategy

89. One of GCHQ's major tasks is leading on the UK's cyber security – protecting Government, the private sector and individuals from those criminals, terrorists and hostile foreign states who use cyber attacks to further their objectives. As such, we have looked at how it is intending to implement the Government's Cyber Security Strategy. GCHQ told us that, in the past, its approach to cyber defence predominantly focused on developing *"high-end national defences… and then just trying to encourage commercial development to take care of the rest"*. However, it has now recognised the importance of confidence in the UK's digital economy, as *"an aggregation of small incidences [would be] damaging to economic prosperity"*. Many such small incidences are due to individuals' failure to use even the simplest good security practices (such as complex passwords). On this, GCHQ is concerned that simply trying to tell people to take greater steps to maintaining security is insufficient, and a more structural approach to defend against low-level attack would be useful: *"we're spending too much time shouting at users and telling them they're too stupid to do the right thing frankly, and that hasn't worked and we need to get away from that"*.[105]

90. The Government and GCHQ call this new approach 'Active Cyber Defence'. This involves taking a proactive approach to the cyber security of the UK, and includes GCHQ assisting private companies in developing automated technological solutions to operate on the underlying internet infrastructure that would prevent a large proportion of cyber attacks from ever reaching end-users. The then Director of GCHQ described the concept of 'Active Cyber Defence' as *"trying to do at a national level what many companies already do, and that's just try to stop a lot of this rubbish getting to the system in the first place"*.[106]

91. GCHQ suggests that it has a unique contribution to make, because *"as throughout history, some of the best information security solutions do come from the state, because of military and intelligence requirements, and because sometimes the research is not economical for the private sector to do"*.[107] GCHQ has also confirmed that it will combine this more hands-on approach with continuing to work proactively with industry to encourage companies to fix security flaws in their products.

I. Individuals bear responsibility for their own cyber security. A large number of cyber attacks succeed because of basic user errors – such as the use of very simple passwords – and these could be prevented if individuals took sensible precautions and followed National Cyber Security Centre advice, which is available on its website.

---

[104] National Cyber Security Strategy 2016–2021*, November 2016.*
[105] *Oral evidence – GCHQ, 19 January 2017.*
[106] *Oral evidence – GCHQ, 19 January 2017.*
[107] *Oral evidence – GCHQ, 19 January 2017.*

J. We welcome GCHQ's work with private companies to improve infrastructure to prevent low-sophistication cyber attacks reaching end-users in the first place.

The Government Response: Organisation

92. In response to the increase in the volume of attacks, and the risk of a major attack on the UK, the Government established the National Cyber Security Centre (NCSC), a public-facing operational unit of GCHQ. This began operation in October 2016, with its new building opening in February 2017. It subsumes the functions of several organisations, including GCHQ's Communications-Electronics Security Group, the UK Computer Emergency Response Team (previously hosted in the Cabinet Office), the cyber sections of the Centre for the Protection of National Infrastructure, and the Centre for Cyber Assessment. NCSC's core staff will be supplemented by secondees from across Government and industry.

93. NCSC's headquarters are in new premises in Victoria in central London, which combine a low-classification working environment (to provide a public-facing role and aid collaboration with industry) with a secure area (to allow NCSC to pull technical capability and expertise from the rest of GCHQ and the wider intelligence community). However, in terms of staff, GCHQ has said that *"roughly half [of GCHQ's NCSC staff], maybe slightly less, will always be in Cheltenham or [or other UK intelligence community locations] because we will always need the high-end cyber defence people and obviously the data that goes with it"*.[108]

94. We expressed concern about the cost of the new NCSC London headquarters (in an expensive new private sector development) compared with the other available options, and as such have asked the National Audit Office for support in reviewing the Government's selection process.

95. GCHQ said the NCSC aims *"to fuse powerful covert capabilities, accesses, data and skills to help provide cyber defence at scale to the UK"*. GCHQ has summarised the NCSC's role as follows:

> *It will be a one stop shop for advice and incident management, not for absolutely everything. So we're not going to be doing all skills across government on the cyber side, we're not going to be doing all policy across government on cyber, it's an operational centre. But a single source of coherent advice on cyber, which is what I think both the private sector and Government really wanted… incident management is not about the NCSC doing everything for everybody. You know, owners of data, lead government departments will still be responsible for their incidents… and of course the link to crime [is really important]. We will have [National Crime Agency] people there… because nearly all cyber… involves crime, sometimes prosecutable but sometimes not. That has to be separate from [an intelligence] organisation like ours, for obvious legal reasons.*[109]

96. More specifically, GCHQ said that NCSC's primary functions are to handle major incidents, provide protective security advice and deliver a new operational strategy for UK cyber security. In terms of major incidents, GCHQ explained NCSC's role as follows:

> *So in the event of a major incident it will be [NCSC's] job to find out as much as it can through covert and overt channels and tell Ministers what we know and it will*

[108] *Oral evidence – GCHQ, 19 January 2017.*
[109] *Oral evidence – GCHQ, 19 January 2017.*

be our job to engage with the victim and provide remedies. That will almost inevitably involve one of our licence providers then going in to use commercial capability to help with the clean-up, because that will be beyond our capabilities at scale. [It] will also involve – in the same way as senior police officers will make assessments… in the event of a major terrorist incident and the Chief Medical Officer and others will advise the public on things relating to public health – in the event of a major [cyber] incident, the definitive position on how many people are affected, what is the risk they're exposed to and what is the mitigating action they can take to protect themselves better will come from us.[110]

97. In terms of its protective security role, GCHQ explained its role as a *"one stop shop"*, replacing a previously diffuse array of Government organisations:

One of the reasons for the Centre was the Governor of the Bank of England asking Ministers at the time [since] he wished to take cyber security more seriously, who did he talk to in Government and the answer was quite clunky… now it is [just the NCSC working with] the Bank of England and that is helpful.[111]

98. On delivering the operational strategy, GCHQ suggested that a central plank will be to leverage GCHQ's expertise to enable and encourage private companies to produce secure products:

There has been quite a significant shift in Government thinking in cyber security, which departs from previous strategies and it also departs from some of the things for example in the US and continental Europe, where a lot of it has just been around high-end national defences, which we concur with and do, and then just trying to encourage commercial development to take care of the rest… Our thinking has moved on to… having technological solutions in the underlying internet infrastructure and how we can develop those.[112]

99. However, since the companies which own the infrastructure cannot be compelled to take the Government's advice, the way in which the NCSC develops strong relationships with companies will be a key part of successfully implementing this new approach. GCHQ is optimistic, and told us that major companies are now very keen to take cyber security issues seriously, suggesting that they are open to assistance from the Government:

I think most companies have now got the message, certainly in the FTSE top 200. All the stats are suggesting they are taking it very seriously… they don't always know what to do, but they are taking it seriously…

So I think it's not that they aren't taking it seriously now, it's what to do about it and what is the balance between what Government can do, delivering it again through the big companies, the [Communications Service Providers], and what can the individual and the company do, and getting that balance we think better is a great experiment. In the past we basically said here we'll give you advice, you go away and do it, but that has been… only successful up to a point.[113]

---

[110] *Oral evidence – GCHQ, 19 January 2017.*
[111] *Oral evidence – GCHQ, 19 January 2017.*
[112] *Oral evidence – GCHQ, 19 January 2017.*
[113] *Oral evidence – GCHQ, 19 January 2017.*

100. Nevertheless, we questioned whether the NCSC should be able to compel computer systems operators to install cyber security of a particular level. GCHQ explained:

> *So within Government, Government will largely do what we ask them to do and, because of the way the Government system has worked, we are the providers of expert advice and we work through it and the Government departments implement it as best they can.*[114]

Whilst that is not the case when it comes to the private sector, some organisations are nevertheless keen for advice, and willing to take action:

> *There isn't any legislation specifically passed to enforce cyber security standards in any sector, including the critical sectors, but it works in different ways in different sectors. If you take finance, one of the most important and certainly one of the top three in terms of attacks, I think it actually works rather well because the Bank of England has interpreted helpfully its statutory remit for financial stability to include cyber security, which seems… reasonable, and so there [is] then a wide discretion to develop relations, which can include cyber security, and… they will consult us and generally take our advice.*
>
> *There are then other regulations. So in civil nuclear, which was topical in the summer with Hinkley Point, the Office of the Nuclear Regulator has the power to direct that certain standards in the engineering must be adhered to and the Office of the Nuclear Regulator consults us on what they should be in the age of cyber defence and that is, I think, a helpful process.*[115]

However, in other areas of the private sector the situation is more complicated:

> *Beyond that, there are areas, because I don't want to mislead you, where it is at least theoretically possible where we could identify a problem in a major national network and say that you need to fix this and they will say, well, that's not affordable or not a priority and so forth…*[116]

Given this problem, we pressed GCHQ as to whether it needed enforcement powers. However, GCHQ argued that the current arrangement was working:

> *There is, in some people's minds, a sort of panacea for this, or at least something called cyber regulatory legislation, which is something that could be reached for. That's obviously a decision for Ministers and there are arguments in both directions. But one of the arguments against is [that] it is generally quite hard to do… in a way that keeps pace with technological change and… in a way that is appropriate across different sectors… In any case there isn't any [legislation] at the moment, so we work across the different sort of legislative contractual frameworks.*[117]

---

[114] *Oral evidence – GCHQ, 19 January 2017.*
[115] *Oral evidence – GCHQ, 19 January 2017.*
[116] *Oral evidence – GCHQ, 19 January 2017.*
[117] *Oral evidence – GCHQ, 19 January 2017.*

101. GCHQ has said that it considers softer measures – including a crossover of staff with relevant industries – to be a more effective way of deepening private sector cooperation:

> *Back to the building for a second though, one of the reasons for having this, as we discussed before, open to industry low classification site, which we can't offer within the secret estate, is precisely so we can have people from finance, from different sectors, sitting in integrated teams…*

Another of the NCSC's approaches involves publishing *"expert, trusted, and independent guidance for UK industry, government departments, the critical national infrastructure and private SMEs"*.[118] Between October 2016 and April 2017, 47 such guidance notes were issued.[119]

The Government Response: Resources

102. As noted previously, the level of resource allocated by Government to cyber-related activities has increased considerably, and it is set to do so still further over the next five years. The National Cyber Security Programme has been given a further £1.9bn to fund its work on *"defending our systems and infrastructure, deterring our adversaries, and developing a whole society capability – from the biggest companies to the individual citizen"*.[120] In 2015/16, GCHQ allocated 24% of its operational effort to cyber security (its single largest category of effort, followed closely by Counter-Terrorism on 23%).

103. However, the continued expansion of cyber-related work is dependent on the Government's ability to recruit and retain cyber specialists. GCHQ previously told us that it struggles to attract and retain a suitable and sufficient cadre of in-house technical specialists because it inevitably has to compete with big technology companies which are able to pay significantly more.[121] In 2013, we were told that GCHQ had implemented more flexible reward packages for technical specialists.[122] Now this has had time to become established, we questioned whether it was having the desired effect. GCHQ informed us that *"[this] has worked up to a point. It stemmed the flow of people going out in particular areas at particular stages of their career"* but that *"we do lose people for salaries. We couldn't possibly compete with four, five times what they are getting from us"*.[123]

104. Despite telling us that they *"can probably never compete purely on salaries"*, GCHQ was relatively optimistic about the overall outlook in skills acquisition, using the value of its unique work as an incentive:

> *We compete on mission, worthwhile work, on interesting work, on variety. If you're a pure mathematician, we're the biggest employer of pure mathematicians in the UK. Going to some of these companies can be quite disappointing. Very well paid, but quite dull… You can go and be an actuary in the City and earn a fortune and use maths, but it won't be quite the same as using maths where we are.*[124]

---

[118] *www.ncsc.gov.uk/guidance.*
[119] *These covered a wide range of subjects including threat intelligence, phishing, ransomware and product security updates.*
[120] National Cyber Security Strategy 2016–2021*, November 2016.*
[121] *ISC Annual Report 2012–2013, HC 547.*
[122] *ISC Annual Report 2012–2013, HC 547.*
[123] *Oral evidence – GCHQ, 8 December 2016.*
[124] *Oral evidence – GCHQ, 8 December 2016.*

GCHQ also told us that to enhance the attractiveness of long-term technical careers, it has created better career paths for technical specialists, including reshaping some senior roles.

105. It also appears that GCHQ has become more comfortable with the fact that it is not going to be able to retain everyone, and has adopted a more open attitude to staying in contact with staff after they leave. GCHQ told us:

> *Our culture in the past has been that once people leave… we never talk to them again and don't let them in the building. I think we have to change that… We can't completely resist the tide… and of course we do want people to go out into the private sector and improve the cyber security industry, for example, in the UK. So losses are not all losses as long as we are getting good people in from the bottom of the organisation, and we are. So I think we have changed our attitude a little bit, that we don't just see everybody leaving as a huge loss.*[125]

106. Nevertheless, staffing remains a problem, and GCHQ spends £***m a year on specialist IT and technology contracts (with associated staff),[126] and a further £71m on 'time hire' contractors (filling in for staff vacancies).[127] GCHQ defended this high level of spend:

> *It gives us a reach into technology that we couldn't possibly… develop and innovation that we couldn't all develop in house, but also gives us flexibility so we can go up and down on headcount if we need to during the year.*[128]

K. Recruiting and retaining technical specialists in the face of ever-growing levels of private sector competition remains a significant challenge: we encourage GCHQ to develop further innovative ways to ensure that it is able to attract and retain the technical staff so critical to its work.

[125] *Oral evidence – GCHQ, 8 December 2016.*
[126] *Oral evidence – GCHQ, 8 December 2016.*
[127] *Written evidence – GCHQ, 18 July 2016.*
[128] *Oral evidence – GCHQ, 8 December 2016.*

SECTION 6: OFFENSIVE CYBER

Offensive cyber covers a range of capabilities, including:

- the ability to retaliate after a cyber attack;
- the capability to deny, disrupt or degrade target communications or weapons systems (including shutting down the source of a cyber attack or in preparation for more traditional military activities); and
- capabilities to attack wider systems or infrastructure – perhaps extending into 'real-world' damage.

Both GCHQ and MOD are responsible for developing these capabilities for the UK and this involves skills and techniques across a range of technical work in each organisation.

Offensive cyber work is broad and includes:

- development of computer code – in plain English what most people would call 'hacking' tools;[129]
- intelligence development (e.g. through interception); and
- delivery (e.g. by network access, or physical access such as through USB).

***. Deployment can take place at different levels, including:

- a specific device, such as a suspect's computer, smartphone or other IT equipment (e.g. to collect information, ***);
- an adversary's computer network (e.g. *** a hostile actor such as ***); and
- ***.

Offensive cyber capabilities are usually highly tailored and system specific, as opposed to a one size fits all 'cyber weapon'.

A widely publicised example of the deployment of offensive cyber capabilities includes the 2009 Stuxnet attack on Iranian uranium enrichment centrifuges, which reprogrammed the control systems to run the equipment in a way that caused physical damage and restricted their ability to successfully enrich uranium. This was the first widely reported use of a cyber weapon causing physical, 'real-world' damage.

UK Offensive Cyber Capability

107. The Government has invested in offensive cyber through the National Offensive Cyber Programme (NOCP), a joint partnership between GCHQ and the Ministry of Defence, established in 2014. In the 2015 Spending Review, the Chancellor described it as the development of *"a dedicated ability to counter-attack in cyberspace"*. GCHQ told us that the programme represents a step change in the UK's effort on offensive cyber:

[129] *GCHQ avoids this term because of the negative connotations associated with it, and instead uses the term computer network exploitation (CNE) to make the distinction between GCHQ's lawful activities and illegal hacking.*

**** this is on a different scale and it is the full spectrum of capabilities from tactical stuff ***... right through to what we would say is the high end of counter state offensive cyber capabilities which might never be used but are the sort [of] high-end deterrents, if you like, and everything in between.*[130]

We note the advantage that the UK's development of a strong offensive cyber capability will confer in terms of an effective deterrent.

108. GCHQ's allocation of effort to developing offensive cyber capabilities has increased very substantially between 2014/15 and 2015/16, from ***% to ***%.[131] We questioned GCHQ on the progress made, in partnership with the Ministry of Defence, on developing the UK's offensive cyber capabilities over the first two years of the seven-year NOCP. GCHQ told us that the programme is split into three tranches, and they had just finished developing the first tranche:

*We… actually over-achieved and delivered [almost double the number of] capabilities [we were aiming for ***]. ***.* [132]

109. There has been a wide spectrum of successes, ***.

Rules of Engagement

110. We questioned GCHQ about its understanding of the legality of offensive cyber attacks. GCHQ told us:

International law applies to state acts in cyberspace in the same way as anywhere else. This is now generally accepted, including at the UN level, although the principle is not laid down in any binding international instrument.

The practice and precedents of how cyber activity ought to be classified under existing international legal principles and concepts [are] underdeveloped. As a result, the application and analysis of existing legal norms to the analysis of cyber activity can vary considerably.[133]

111. One of the problems is the difficulty of attributing cyber attacks – and even where they can be technically attributed, proving this to an international legal standard without revealing sensitive capabilities or accesses is generally not possible. GCHQ told us:

****. It's not like arms control, where you can point to something and say they've breached the rules and we can attribute this activity to this person.*[134]

112. As the use of offensive cyber inevitably becomes more widespread, further work will be required to develop a better international consensus on the rules of engagement for offensive cyber. GCHQ told us that it supported this concept in principle, but held some concerns, for example about others' adherence to such agreements: *"***."* [135]

113. Despite these difficulties, the UK has played a major role in seeking international agreements in this area, particularly through the recurring Global Conference on

[130] *Oral evidence – GCHQ, 19 January 2017.*
[131] *Written evidence – GCHQ, 18 July 2016.*
[132] *Oral evidence – GCHQ, 19 January 2017.*
[133] *Written evidence – GCHQ, 27 February 2017.*
[134] *Oral evidence – GCHQ, 19 January 2017.*
[135] *Oral evidence – GCHQ, 19 January 2017.*

Cyberspace. This event brings together governments, the private sector and civil society to support practical cooperation, promote the exchange of knowledge and discuss norms for responsible behaviour in cyberspace. The conference was first established in London in 2011 and has since been hosted in Budapest, Seoul and The Hague.

L. We recognise the importance of offensive cyber capabilities for the national security of the UK, although it will be important in the future to seek international consensus on the rules of engagement and we would support Government attempts to establish this.

SECTION 7: THE INTELLIGENCE COVERAGE AND EFFECTS PLAN

114. SIS and GCHQ priorities are now determined centrally via the Intelligence Coverage and Effects (ICE) Plan. The ICE Plan, introduced in 2016/17, replaces the Priorities for Intelligence Coverage, which were previously set by the Joint Intelligence Committee. The National Security Secretariat (NSS) is responsible for coordinating the annual ICE process, which runs from January to April – with the ICE Plan itself being agreed by the National Security Council (NSC) in May/June.

115. As its name suggests, the ICE Plan includes both intelligence coverage and intelligence effects:

- 'coverage' is the collection of information (or acquisition of information from allied intelligence services) by the Agencies; and
- 'effects' describes the Agencies' engagement in activities which have 'real-world' outcomes (e.g. disrupting terrorist plots or preventing the spread of nuclear weapons).

116. The ICE Plan delineates the themes on which there are intelligence requirements. The *** themes listed in May 2016 are as follows:

ICE Plan themes	
• Counter Terrorism • Counter Proliferation • Cyber • Hostile Foreign Activity • Serious Organised Crime • Leadership & Political • Conflict & Stability	• Sanctions • Military Capabilities • Defence Technology • Support to Military Operations ***

117. In addition to themes, the ICE Plan also prioritises the various countries, regions and organisations against which there are intelligence requirements. Against those countries, regions or organisations listed as High or Medium priority, the ICE Plan marks them against the themes on which there are intelligence requirements. The prioritisation agreed by the NSC in May 2016 is as follows:

May 2016 ICE Plan prioritisation				
High priority		**Medium priority**	**Low priority**	
***	***	***	***	***
***	***	***	***	***
***	***	***	***	***

***	***	***	***	***
***	***	***	***	***
***	***	***	***	***
***	***	***	***	***
***	***	***	***	***
***	***	***	***	***
***	***	***	***	***
***	***	***	***	***
***		***	***	***

118. The ICE Plan is monitored by the ICE Steering Group, which meets quarterly and comprises senior officials from the Agencies' main customer Departments, headed by the Chair of the Joint Intelligence Committee. According to NSS, the Steering Group aims to:

> *1. ensure that performance by [SIS and GCHQ] against ICE targets is on track;*
>
> *2. review any in-year pressures on the annual ICE Plan, triggered by changes in strategy, directions from the NSC, or driven by events, with resource allocations amended if necessary;*
>
> *3. monitor long-term or future ICE requirements and access development tasks; and*
>
> *4. agree any proposed changes to the shape and extent of the ICE process itself.*[136]

119. In relation to monitoring the performance of SIS and GCHQ in delivering against the ICE Plan, the Acting Chair of the Joint Intelligence Committee conceded that – despite the work done by SIS and GCHQ to improve the monitoring of the impact of their work – measurement was by its very nature difficult. He accepted that merely counting intelligence reports was too simplistic, telling us that *"we need to introduce… more of the qualitative side… we need to [evolve] the process so that we can also look at the extent to which… it is not just about volume; it is about quality"*.[137]

120. The Acting Chair also told us that even though the ICE Plan is produced annually, it is not set in stone for the year, and that there have been some in-year changes to the 2016/17 ICE Plan: *"it was clear that *** was an area which needed more attention and that was reflected to the Agencies at the mid-year point"* and *"similarly *** [is] emerging [as a] bigger problem than people thought"*.[138] The following section considers some of the key geographical ICE priorities.

[136] *Written evidence – NSS, 31 October 2016.*
[137] *Oral evidence – JIO, 2 February 2017.*
[138] *Oral evidence – JIO, 2 February 2017.*

SECTION 8: COUNTRIES OF INTELLIGENCE AND SECURITY INTEREST

121. Whilst the geographical element of the ICE Plan sets SIS and GCHQ's priorities for intelligence collection, and does not bind MI5, there is nevertheless a natural read-across to MI5's work countering Hostile State Activity in the UK. The two workstreams – counter-espionage and intelligence gathering on nation states – have become increasingly interwoven given the extent of joint working between the Agencies, and are therefore dealt with together in this section.

Allocation of Effort

122. MI5's work on Hostile State Activity, including counter-espionage, counter-proliferation and protective security, accounts for around 18% of its overall effort. This might appear low compared with effort directed against international and Northern Ireland-related terrorism (82%); MI5 has, however, explained – using Russia as an example – that such percentages are somewhat misleading as they do not reflect the significant increase in MI5's size over recent years:

> *In terms of headcount [MI5 has] *** people doing Russia ***. Back in Cold War days, MI5 was ***, and we are 4,000 going to 5,000 today.*[139]

123. The Home Secretary also noted that the division between staff working on International Counter-Terrorism and Hostile State Activity can be fluid: MI5's international counter-terrorism effort *"includes Hostile Foreign Activity… where it impacts on potential counter-terrorism activity"*.[140]

124. In terms of SIS and GCHQ's effort on intelligence collection, SIS allocates around two-thirds of its effort against nation states, and GCHQ a little under half (alongside 24% of its effort being on protective cyber security, which covers both state and non-state cyber threats).

Responsibility

125. Overall policy (as opposed to operational) responsibility for countering Hostile State Activity in the UK sits in the National Security Secretariat in the Cabinet Office. We have queried why this is the case: the Home Office is the policy department responsible for MI5, which is the Agency predominantly focused on this threat. On this, the Office for Security and Counter-Terrorism (OSCT) informed the Committee as follows:

> *I think [Hostile State Activity] is really interesting and there is a big push now across Government on that… It is being run out of Cabinet Office and I think… we will see over time… whether that then emerges and is reallocated at some stage. Its natural home, within a Department of State, clearly would be the Home Office but that is not how it is at the moment.*[141]

[139] *Oral evidence – MI5, 1 December 2016.*
[140] *Oral evidence – Home Secretary, 2 March 2017.*
[141] *Oral evidence – OSCT, 3 November 2016.*

126. When asked why Cabinet Office had policy responsibility for Hostile State Activity, the former National Security Adviser noted: *"I have never felt any particular sort of duplication."*[142]

M. We note that day-to-day policy responsibility for Hostile State Activity sits with the National Security Secretariat in the Cabinet Office, even though it primarily holds a coordinating function rather than one of policy and delivery. This is symptomatic of the increasing centralisation of intelligence and security matters, which is an issue that continues to cause us concern. Policy on Hostile State Activity may fit more naturally with the rest of domestic-orientated national security policy in the Office for Security and Counter-Terrorism in the Home Office.

Russia

127. Russia – and, previously, the Soviet Union – has been a focus for the Agencies for many years. After the end of the Cold War, the allocation of effort on Russia and the former Soviet Union decreased in line with the perceived reduction in threat. However, the past decade has seen a resurgence in the threat, with activities including the illegal annexation of Crimea, engagement in military conflict elsewhere in the world, and cyber attacks against Western countries.

128. Russia *** is a *** priority under the ICE Plan, and is of intelligence interest across *** themes – ***. This is clearly reflected in the Agencies' allocations of effort: ***. The Acting Chair of the Joint Intelligence Committee (JIC) informed us that *"Russia has risen up the agenda"*[143] during 2016/17, ***.[144]

129. Defence Intelligence (DI) has also considerably increased its focus on Russia recently, informing us that ***.[145] In terms of Hostile State Activity work, MI5 has said that Russia is ***.

UK aims and challenges in working against Russia

130. In terms of Russia, among SIS and GCHQ's priorities is understanding the Kremlin's objectives and intentions. The Chief of SIS informed us that *"***"*[146] and GCHQ said *"***"*. MI5's main aim is countering Russian Intelligence Service activity in the UK in order to protect the UK Government and industry from espionage and to counter Russian influencing operations.[147]

131. Understanding Russian military capabilities is another important requirement. ***.[148]

132. GCHQ informed us that ***.[149]

---

[142] *Oral evidence – NSS, 13 October 2016.*
[143] *Oral evidence – JIO, 2 February 2016.*
[144] *Oral evidence – GCHQ, 8 December 2016.*
[145] *Oral evidence – DI, 7 July 2016.*
[146] *Oral evidence – SIS, 17 November 2016.*
[147] *Written evidence – GCHQ, 31 October 2016.*
[148] *Oral evidence – SIS, 17 November 2016.*
[149] *Oral evidence – GCHQ, 8 December 2016.*

133. This reads across to Russia's activities in Eastern Europe. SIS has recently informed us that *"***"*.[150] ***, and that Russia is to all intents and purposes in conflict with Ukraine:

> ***.[151]

134. For DI, Russian actions in the Middle East are a further cause for concern. Its staff will be *"supporting and be part of an integrated effort reporting on [ISIL] and the Russian inputs [in the region]"*.[152]

135. ***.[153]

136. More generally, SIS has described the Russian state as *"formidable adversaries"*. ***.[154]

137. However, MI5 caveated this, saying that ***.[155]

N. The events of the past decade or so show that the threat from Russia remains significant. The Agencies' focus on Russia must be maintained.

Russian objectives and activity against UK and allied interests

138. On Russian activity against the UK, GCHQ has informed us that *"***"*.[156] However, Russia's objectives in individual attacks may seem obscure: some commentators have speculated that certain cyber attacks which have been widely reported in the media as being Russian – most notably the hacking of US Central Command's Twitter account and the more substantial attack against TV5Monde in April 2015 – have been 'false-flagged' as Islamist extremist attacks.[157] It is possible that Russia is ostentatiously flexing its muscles towards the West under a deliberately thin blanket of deniability, or these may simply be providing a useful public cover for the Russian agencies' practice runs. GCHQ said:

> ***.[158]

139. GCHQ has also said ***.[159]

---

[150] *Written evidence – SIS, 31 January 2017.*
[151] *Written evidence – SIS, 3 August 2016.*
[152] *Oral evidence – DI, 7 July 2016.*
[153] *Written evidence – GCHQ, 31 October 2016; oral evidence – SIS, 17 November 2016.*
[154] *Oral evidence – SIS, 17 November 2016.*
[155] *Oral evidence – MI5, 1 December 2016.*
[156] *Oral evidence – GCHQ, 19 January 2017.*
[157] *'Russian hackers accused of attacks on Bundestag and French TV broadcaster',* The Telegraph*, 29 October 2017.*
[158] *Oral evidence – GCHQ, 19 January 2017.*
[159] *Oral evidence – GCHQ, 19 January 2017.*

140. It appears that Russia has a high-risk tolerance, and is not targeted in its use of offensive cyber capabilities. In the cyber world, DI informed us that in Russia *"the risk appetite is quite different and they are quite prepared to use the world as a range, [saying] 'we will give it a go and see what happens' "*.[160] Equally, MI5 has said in relation to stories about potential Russian cyber interferences in the Democratic National Committee:

> **** they clearly are operating to risk thresholds which are nothing like those that the West operates.*
>
> ***.[161]

141. It has been reported that cyber attacks such as that on the Democratic National Committee are part of a wider Russian operation to disrupt and agitate Western political discourse – an operation which includes more traditional subversion, propaganda and disinformation campaigns.[162] It is also possible that the false-flagging of cyber attacks to Islamist extremist groups is an attempt to promote fear and discord in the West. We asked MI5 about these issues and were told:

> ***.[163]

142. SIS informed us that *"all three Russian intelligence services are tasked with carrying out 'information operations' [which] goes beyond promulgating the Russian perspective and includes the creating and propagation of forgeries and falsehoods"*. One obvious area is Ukraine, where:

> *Russia conducts information warfare on a massive scale... An early example of this was a hugely intensive, multi-channel propaganda effort to persuade the world that Russia bore no responsibility for the shooting down of [Malaysian Airlines flight] MH-17 (an outright falsehood: we know beyond any reasonable doubt that the Russian military supplied and subsequently recovered the missile launcher).*[164]

143. Serious Russian disinformation campaigns are also found across Europe: ***.[165] One particularly notable case, which has been widely reported as an attempt to interfere in German politics, was the so-called 'Lisa case'. According to Reuters:

> *Moscow's intervention in an alleged rape case involving a German-Russian girl has heightened suspicions in Berlin that it is trying to stir up trouble, with a view to weakening Chancellor Angela Merkel.*[166]

144. GCHQ sees this type of interference as being likely to continue and to grow:

> *Russia has… in Europe [tried] to influence opinion, not necessarily through cyber, through all sorts of other traditional methods, and I think it's about thinking through… how you would influence a particular constituency to agree with a different direction, and it might not… be through cyber attack or stealing data, it*

---

[160] *Oral evidence – DI, 7 July 2016.*
[161] *Oral evidence – MI5, 1 December 2016.*
[162] *US Intelligence Community Assessment,* Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 6 January 2017.*
[163] *Oral evidence – MI5, 1 December 2016.*
[164] *Written evidence – SIS, 30 August 2016.*
[165] *Written evidence – SIS, 30 August 2016.*
[166] *Reuters, 'German-Russian ties feel Cold War-style chill over rape case', 1 February 2016.*

might be through rather more basic influencing campaigns as we've seen Russia engage in over the many many years.[167]

Liaison with Russia on intelligence and security matters

145. Whilst Russia clearly represents a major threat, there are also areas of mutual intelligence and security interest – most notably around counter-terrorism and Syria. Restrictions on liaison with Russia on intelligence matters were introduced following the murder of Alexander Litvinenko, but in May 2013 the then Foreign Secretary wrote to the Committee to inform it that a channel of communication had been reopened with the FSB (Russia's domestic security service) in relation to security measures for the Sochi Winter Olympics. The Foreign Secretary wrote that:

***.[168]

146. SIS informed us that it currently has ***. SIS said:

***.[169]

***.[170]

147. ***.[171]

O. Whilst collaboration with Russia on matters of mutual intelligence interest would be difficult, we agree with SIS that limited lines of communication should be maintained, although a delicate balance is needed.

China

UK aims and challenges in working against China

148. ***. The Agencies' aims against China are relatively similar to those against Russia: ***.[172]

149. ***.[173] SIS and GCHQ's main aims are to understand China's objectives and intentions, and to support MI5 in countering Chinese Intelligence Service activity against UK interests ***.

Chinese objectives and activity against UK and allied interests

150. A great deal of China's intelligence aims against the UK are for economic motives, in addition to attempting to acquire classified government and military material. According to GCHQ, China's cyber capability *** has enabled it to have greater successes:

***.[174]

---

[167] *Oral evidence – GCHQ, 19 January 2017.*
[168] *Written evidence – Foreign Secretary, 9 May 2013.*
[169] *Oral evidence – SIS, 17 November 2016.*
[170] *Oral evidence – SIS, 17 November 2016.*
[171] *Written evidence – SIS, 18 August 2017.*
[172] *Oral evidence – SIS, 17 November 2016.*
[173] *Oral evidence – MI5, 1 December 2016.*
[174] *Oral evidence – GCHQ, 19 January 2017.*

151. GCHQ also informed us that the Chinese *"weren't bothered for a while about being attributed in generic terms by the US and others as major cyber stealers of information"*, but *"that is beginning to change a little bit… ***"*.[175] As part of the diplomatic push to curb cyber crime, in October 2015 the UK and China jointly announced that they had agreed not to engage in commercial cyber espionage on one another. GCHQ said:

> ***.[176]

***.[177]

China and the UK's Critical National Infrastructure

152. Chinese involvement in the UK's Critical National Infrastructure has for a long time been a point of concern. In June 2013, the Committee published its report *Foreign Involvement in the Critical National Infrastructure*, which covered the role of the Chinese company Huawei in the UK's telephone infrastructure; in response to this, the Government set up an Oversight Board for Huawei's Cyber Security Evaluation Centre, which continues to report annually.

153. More recently, there has been public controversy about the granting of a role to the Chinese State in the financing of the new Hinkley Point C nuclear power station. ***: GCHQ said that *"we did see some commentary that the review of the Hinkley decision was prompted by the intelligence community and that wasn't the case"*. The Director elaborated on GCHQ and MI5's involvement in the review:

> ***.[178]

P. We understand that China's role in relation to Hinkley Point is primarily one of financing, and that operational control remains in UK hands. Nonetheless, we note that the Agencies were consulted in the making of this decision.

Liaison with China on intelligence and security matters

154. In terms of intelligence cooperation, SIS does have some contact with the Chinese Ministry of State Security: *"the… relationship… continues to develop; ***"*.[179] More generally, SIS informed us that it is keen to establish links with the Chinese security establishment:

> *Now, self-evidently we need to do that in a way that preserves our laws and values…* ***.[180]

[175] *Oral evidence – GCHQ, 19 January 2017.*
[176] *Oral evidence – GCHQ, 19 January 2017.*
[177] *Written evidence – GCHQ, 2 June 2017.*
[178] *Oral evidence – GCHQ, 19 January 2017.*
[179] *Written evidence – SIS, 31 January 2017.*
[180] *Oral evidence – SIS, 17 November 2016.*

Iran

155. Iran is considered a *** priority in the ICE Plan, marked as relevant against *** themes. This is reflected by ***: SIS had *** staff working on Iran ***, and GCHQ had a broadly similar number (***).

156. Iranian motivations against the UK are more obscure than those of Russia and China. GCHQ has suggested that Iran is primarily attempting a show of strength:

> ***.[181]

157. The Agencies' primary concern in relation to Iran has been counter-proliferation. At its peak, ***, they were allocating ***% of their effort to counter-proliferation work, although SIS has informed us that this is reducing in the wake of the Iranian nuclear deal of July 2015:

> ***.[182]

***.[183]

North Korea

158. North Korea remains a significant adversary for the Agencies, being a *** priority under the ICE Plan and marked as relevant against *** themes. ***.

159. North Korea's objectives against the West are a mixture of statecraft and economics, albeit that its economic attacks are reported to be a much cruder form of theft than China's work against Western intellectual property; for example, widespread media reports have suggested that, in February 2016, North Korea stole $101m from the Bangladesh Bank via the SWIFT electronic payments system. On North Korea's attacks, GCHQ said: *"they are very focused on the things they most care about, ***"*.[184]

160. It has been widely reported that North Korea conducted a major successful cyber attack against Sony Pictures in the USA in late 2014. GCHQ has informed us that there is significant risk of a similar attack on the UK:

> ***.[185]

161. North Korea's recklessness and unpredictability, as possibly demonstrated by the Sony hack, is a significant difficulty in defending against its attacks: it is prepared to use its capabilities without any concern for attribution, and for ideological motives which are alien to other countries. Additionally, the lack of legal process means that North Korea can act with considerable speed. As GCHQ put it:

> ***.[186]

---

[181] *Oral evidence – SIS, 17 November 2016.*
[182] *Oral evidence – SIS, 17 November 2016.*
[183] *Oral evidence – SIS, 17 November 2016.*
[184] *Oral evidence – GCHQ, 19 January 2017.*
[185] *Oral evidence – GCHQ, 19 January 2017.*
[186] *Oral evidence – GCHQ, 19 January 2017.*

Other Countries

162. There are various other countries marked as high priority under the ICE Plan: ***. In reality, many of these countries are of much lower priority than the very highest priority States (***), and have commensurately fewer themes marked against them in the ICE Plan.

163. ***.[187]

164. ***.[188]

165. ***.

[187] *Written evidence – SIS, 30 August 2016.*
[188] *Written evidence – SIS, 30 August 2016; oral evidence – SIS, 17 November 2016.*

SECTION 9: INTERNATIONAL RELATIONSHIPS

Five Eyes

166. The Five Eyes – consisting of the UK, USA, Canada, Australia and New Zealand – is the closest international intelligence partnership in the world. The Agencies frequently refer to the importance of Five Eyes assistance in their routine reporting to us.

167. Throughout 2016/17, as a Committee we have had significant interaction with our American and Canadian counterparts and the intelligence communities they oversee, and have examined aspects of the UK's relationships with these countries.

USA

168. We visited Washington in September 2016, meeting the Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. We also spoke to various Washington-based staff from the UK Agencies. The closeness of the relationship between the UK and US agencies – and the value that both sides place upon it – was apparent throughout our visit.

169. Our visit took place prior to the election of President Trump. Certain views that the President has expressed – particularly prior to his election – have the potential, if they were to become official policy, to pose difficulties for the UK–USA intelligence relationship. These include, *inter alia*, the potential for a change in the US relationship with Russia and Iran, and a change in policy on the use of torture and cruel, inhuman or degrading treatment. Given the close joint working on intelligence issues, we have asked the Agencies for their assessment of the situation. GCHQ has expressed a measured view:

> *I think it's early days and obviously if some of the more extreme talk in the campaign was translated into policy or legislation, then that would be difficult… But we have no reason to think that will happen. I think the most important thing for us is that we know what's going on, and that our staff continue to talk to each other, our lawyers continue to talk to each other and that we are aware of any fundamental changes in the legal position, but there's no reason to expect any…*[189]

170. SIS has also expressed a cautious approach towards prematurely drawing conclusions on the impact of a Trump presidency:

> *If something happened which caused us fundamentally to revisit our presumption of legality [of the US agencies' actions], which we have got now, hard won after many years after all the problems we have discussed [on detainee treatment and rendition], then that would be really difficult. But emphatically I am not assuming that is going to happen. We are many steps away from that and I think there are lots of good reasons why it would not. ***.*[190]

[189] *Oral evidence – GCHQ, 8 December 2016.*
[190] *Oral evidence – SIS, 17 November 2016.*

171. Asked about statements made by President Trump during the election campaign,[191] MI5 was quite clear:

> *Whether this signals a likelihood to return to forms of abuse of detainees, I think we spent enough time in this room talking about that for you to know I would be very highly alert to any sort of changes like that. I have communicated internally already about this in MI5, that, you know, whatever happens, MI5 will operate within the law and by our values. So if any of that changes on the US side, there will be a consequence in the relationship but, you know, we will not collude in any sort of change in that sort of behaviour. Of course we won't. But let's not assume that is going to happen in the US.*[192]

Q. Any significant change in US policies relating to detainee treatment would pose very serious questions for the UK–USA intelligence relationship. The US agencies are well aware of the implications for cooperation with the UK and other allies, and the UK Agencies are monitoring the situation closely. The UK Government must continue to keep a close eye on any changes in US policy and take swift action if there are signs that these might run counter to British laws and values.

172. In its *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, published in November 2014, the Committee expressed serious concern about the difficulties experienced by UK Agencies in obtaining content from US communications service providers (CSPs). The Committee urged the Government to use its close intelligence relationship to lobby for legislative change in the USA that would allow the CSPs to comply with UK warrants.

173. In response to this, the Prime Minister appointed Sir Nigel Sheinwald as Special Envoy to the USA on Intelligence and Law Enforcement Data Sharing in September 2014. In March 2015, Sir Nigel submitted a classified report to the Prime Minister, which concluded that a new international framework should be created to enable data sharing between countries with appropriately high standards of oversight and privacy protection (***). Following this, in July 2016 a US Bill was submitted to Congress which would enable international data sharing of this type.

174. The Bill had not been introduced in sufficient time to enable it to pass through Congress before the US election, but, from our discussions with both Congressional intelligence committees and the US agencies, it is our view that there is significant political will in Washington for this legislation to proceed. We note that, during a Senate sub-committee hearing on the Bill, Senators from both parties expressed their strong support and pledged their *"best efforts"*.[193]

175. The National Security Secretariat (NSS) has also explained that the proposed US legislation will permit – but not oblige – US CSPs to comply with UK warrants. At the moment, US CSPs are not permitted under US law to provide data to foreign governments except in very specific circumstances.[194] The removal of the legislative bar is only the first

---

[191] *For example,* Washington Post *(17 February 2016) reported that presidential candidate Trump, during an election campaign event, said: "Don't tell me it doesn't work – torture works."*

[192] *Oral evidence – MI5, 1 December 2016.*

[193] *www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights*

[194] *One such circumstance would be the use of the UK–US Mutual Legal Assistance Treaty, although this is only available for use in criminal prosecutions as opposed to intelligence gathering. In addition, the US Electronic Communications Privacy Act permits CSPs to disclose user information to UK authorities where*

step; the next step will be a bilateral agreement on data sharing between the two Governments setting out the standards that must be adhered to, and the circumstances in which requests for data can be made. This will be accompanied by discussions with the companies themselves (which we are told has been done *"with a number of companies"* already) to ensure that the CSPs are able to cooperate under this agreement, which NSS states *"relies on the companies being in a space to cooperate and feeling that they have confidence in the legal system in the US and here, and in the agreement"*.[195]

R. We are encouraged that the Government has taken forward this Committee's recommendation on data sharing with US communications service providers. We are, however, concerned at the length of time it is taking to make progress. Given the goodwill towards this legislation, which the Committee discerned on its visit to Washington, we urge the Government to renew efforts to pursue this matter with its US partners.

Canada and Australia

176. The Committee has this year engaged with the Canadian Government and Parliament, as the Canadians establish a parliamentary committee equivalent to the ISC for the first time. We have met the Canadian Minister for Public Safety and the Chair-designate of the new Canadian committee in London and in Ottawa, and submitted written information on the UK system.

177. The establishment of the new committee was a major topic of discussion for the Committee when it visited Ottawa in September 2016. In addition to the meetings noted above, we also met a number of parliamentarians, the Canadian Security Intelligence Service, Communications Security Establishment (CSE), Royal Canadian Mounted Police, the Security Intelligence Review Committee and the CSE Commissioner.

178. Australia is currently conducting an independent review of its intelligence community. We met the intelligence review team, which included Sir Iain Lobban, the former Director of GCHQ, and provided our insights – primarily on oversight aspects.

European Partners and Brexit

179. Whilst none are as deep as the Five Eyes, the Agencies nonetheless have significant relationships with other countries. In particular, several areas of obvious shared intelligence interest exist with our European allies – primarily on International Counter-Terrorism but also on other Hostile State Activity and Serious and Organised Crime.

180. Since the Brexit referendum on 23 June 2016, we have looked at the risk, in general terms, as to the national security implications of Brexit for the work of the organisations that we oversee. A number of high-profile former Heads of Agencies have publicly expressed their concerns regarding Brexit. Lord Evans of Weardale, the former Director General of MI5, and Sir John Sawers, the former Chief of SIS, wrote a public article in which they stated that, despite national security being clearly set out as a national responsibility within the Lisbon Treaty, *"the EU still matters to the UK's security"*.[196]

---

they have a good faith belief that an emergency involving death or serious physical injury to any person requires disclosure without delay.

[195] *Oral evidence – NSS, 13 October 2016.*

[196] *Jonathan Evans and John Sawers,* Sunday Times*, 8 May 2016.*

They also highlighted the impact of leaving the EU on the availability of the data that is so essential to the work of the intelligence Agencies.

181. In their evidence to this Committee, the Heads of the Agencies have also hinted at a number of areas where Brexit will make their work more complicated. When we asked the Director General of MI5 if he was confident that Brexit will not affect the UK's mutually beneficial relationships with European security agencies, he replied:

> *Yes and no. There are two parts to this. My life has got more difficult since the referendum because of the need to invest reassurance time with all of our European partners, but the thing that is driving the quality of those relationships currently is the darkness of the threat and the common concern about it. Half of Europe is scared of terrorism and the other half is scared of Russia and both halves want us to help them… So that will not change with Brexit because Article 4.2 [of the Lisbon Treaty] had all of that outside scope anyway.*
>
> *My hesitancy… is because there are a whole bunch of issues which are within EU competence that will affect, depending how they come out in the negotiation, will affect our ability to operate in the European space… [We] could be affected… in areas like data sharing, what happens with borders… what happens with law enforcement cooperation…*
>
> *There is a bit of uncertainty attached to it because those are all things that are part of negotiation that we are nowhere near yet so there is a bit of a question mark for me. So a mixed picture I guess.*[197]

182. We have asked the Agencies how Brexit could affect their relationships with European partners. GCHQ reiterated the importance of these relationships, but was relaxed about the direct implications:

> *I think all our partnerships have been bilateral over the years. So we have never done anything through the European institutions, except some cyber security advice… we have talked before about [improved SIGINT sharing] which we have helped to establish [in Europe with key partners] all contributing SIGINT data, and that is still… finding its way, but its huge potential is based on what we [have done previously] but focused on terrorism and ISIL, and really good, but not in any way connected with the European institutions. So there is no reason why it would be affected by Brexit.*[198]

However, GCHQ did have concerns as to how European data sharing would work after Brexit:

> *The only area where I think there will be some implications, yet to be decided, is on data legislation and how that develops. I imagine, once we are not part of the EU, there will need to be some provision, as the US have with their privacy shield, or whatever it was called, Safe Harbour, because… companies, the big companies, will need to be able to share data in a way that is legally compliant on… both sides, the UK and the EU. That's a policy issue way beyond intelligence, actually, but it will have big implications for us, so getting that right is important.*[199]

---

[197] *Oral evidence – MI5, 1 December 2016.*
[198] *Oral evidence – GCHQ, 8 December 2016.*
[199] *Oral evidence – GCHQ, 8 December 2016.*

183. The Government has publicly acknowledged the importance of EU tools and mechanisms for keeping the UK safe and secure, and that agreements will need to be reached around these in the negotiations to come:

- In the first Annual Report of the 2015 National Security Strategy, the Government stated: *"EU tools and measures, which enable information sharing and facilitate practical cooperation between law enforcement and security agencies, play an important role as enables for tackling serious crime, securing borders and combatting terrorism. We will need to reach agreement on a range of issues such as these in the negotiations."* [200]
- In the Brexit White Paper, the Government lays out examples of a number of EU mechanisms and tools that are currently heavily used by the UK, including:
    - the significant UK involvement with Europol;
    - the 8,000 individuals extradited in 2015/16 using the European Arrest Warrant;
    - the significant use of the Schengen Information System II, which includes alerts for wanted or suspected criminals (collectively 13,000 alerts); and
    - the fact that the UK is the fourth largest user of the European Criminal Records Information System.

184. We have also discussed Brexit – amongst other issues – in bilateral discussions in Paris with our French counterpart committee, as well as the members of the intelligence community they oversee. Our interlocutors expressed some concerns about aspects of cooperation becoming more difficult after Brexit, but they appeared to value their collaboration with the UK greatly and expressed a wish for it to continue unabated after Brexit.

185. Given the serious concerns expressed about the impact of Brexit on European security (in general) and on the security of the UK (specifically), we initially asked MI5 and GCHQ for a written assessment of the potential national security implications of Brexit. They each referred us to the Cabinet Office for a response, stating that negotiation issues were a political matter. However, the Cabinet Office declined to provide any information further to that already contained in the Brexit White Paper. Whilst we accept that the Brexit negotiating strategy is not a matter for this Committee, the decision to leave the EU clearly has direct and indirect implications for the work of the Agencies – and these are well within this Committee's remit. We therefore disagree that this is purely a political matter.

S. European mechanisms play an essential role in the UK's national security, particularly at a time when the Agencies have all emphasised the importance of enhancing their cooperation with European counterparts. We urge the Government to be more forthcoming with its assessment of the associated risks of the UK's impending departure from the European Union, and the mitigations it is putting in place to protect this vital capability.

[200] *First Annual Report of the National Security Strategy and Strategic Defence and Security Review 2015.*

T. In particular, it is in the overall interests of European security that the UK Agencies retain full access to European data sources and continue cooperation on law enforcement and intelligence. Ensuring that such access and cooperation can continue post-Brexit should be a priority for both the UK and the EU. Once the UK has left the EU, intelligence cooperation is an area where it can continue to be a leader amongst its European allies.

SECTION 10: ADMINISTRATION AND EXPENDITURE

186. The 2015 National Security Strategy and Strategic Defence and Security Review (SDSR) committed an extra £2.6bn over five years to the intelligence and security Agencies to ensure that *"they have the resources and information they need to prevent and disrupt plots against this country at every stage"*.[201] Nearly half of this comes from a 17% real terms increase in annual budget over five years. However, it should be noted that just over half of this total is to be found by the Agencies themselves through extremely demanding savings and efficiency targets.

187. As a consequence of this additional funding, the Agencies have developed a strategy for where they will prioritise investment over the Spending Review period. The joint *Security and Intelligence Agencies' Plan* aims to deliver:

- *recruiting and training an additional 1,900 intelligence and analytical staff across the three agencies;*
- *increasing resources to pursue terrorists;*
- *creating a bigger and more capable global security and intelligence network to protect British citizens at home and abroad, and work with our partners;*
- *investing in capabilities to detect and analyse cyber threats, pre-empt attacks and track down those responsible;*
- *developing a series of measures to actively defend ourselves against cyber-attacks;*
- *creating a new National Cyber Security Centre to lead the response to cyber incident management; and*
- *helping companies and the public to do more to protect their own data from cyber threats.*[202]

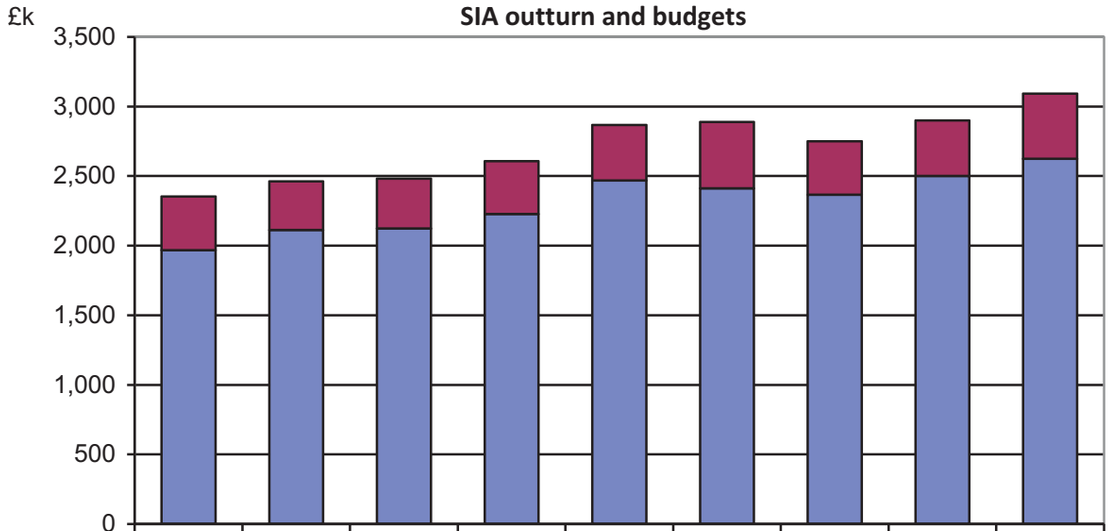
188. This additional investment comes at a time of budget cuts for the majority of government departments. However, as noted in the previous sections of this Report, we agree that such investment is warranted to ensure that the intelligence and security community is suitably equipped to address the current set of challenges. That being said, the current economic climate places an ever greater imperative on ensuring that this additional funding is used efficiently and effectively to deliver the outcomes it is allocated for, and not absorbed by financial mismanagement or inefficiency.

Single Intelligence Account

189. The Single Intelligence Account (SIA) is the money voted by Parliament to fund the work of the Agencies.[203] The chart below shows the SIA over the last five years and

[201] National Security Strategy and Strategic Defence and Security Review 2015.
[202] Security and Intelligence Agencies' Plan 2016–2021.
[203] *All financial figures included in this Report have been provided by and verified by the Agencies.*

through to the end of the current Spending Review period in 2019/20.[204] Whilst there are small fluctuations from year to year (typically due to accounting adjustments for depreciation and revaluations), there is clearly a general upward trend. Over the period from 2011/12 to 2019/20, resource budgets are expected to increase by 33% and capital budgets by almost 22% (not accounting for inflation). This is notable in the general climate of significant cuts in Government spending: the Agencies are one of very few parts of Government where budgets are increasing.



	2011/12 (outturn)	2012/13 (outturn)	2013/14 (outturn)	2014/15 (outturn)	2015/16 (outturn)	2016/17 (planned)	2017/18 (planned)	2018/19 (planned)	2019/20 (planned)
Capital	385,357	347,886	358,138	378,959	398,506	476,670	384,000	400,000	469,000
Resource	1,968,626	2,113,758	2,123,469	2,228,142	2,469,085	2,412,818	2,366,118	2,500,334	2,623,556

190. In 2015/16, the allocation between the three Agencies (including a small proportion which is used to fund central functions within the Cabinet Office) was as follows:

£m (%)	MI5	SIS	GCHQ	Central	TOTAL
2015/16	*** (***%)	*** (***%)	*** (***%)	*** (***%)	2,868 (100%)

Transparency

191. The annual SIA Financial Statement provides a helpful overview of the total spending on the intelligence Agencies.[205] However, it is the only budgetary information on the Agencies that is published; the division of the Single Intelligence Account between the three Agencies is not published for national security reasons.

192. The ISC has for many years questioned this practice, on the basis that any potential harm caused should be outweighed by the benefits of greater transparency. Last year, the then National Security Adviser, Sir Mark Lyall Grant, agreed, saying that as long as detailed information on specific areas of work remained classified it should be possible to

[204] *SIA Financial Statement 2015/16, HC 363, 14 July 2016. Budgets shown in the chart are a total of Departmental Expenditure Limits (DEL) and Annually Managed Expenditure (AME), inclusive of depreciation.*
[205] *SIA Financial Statement 2015/16, HC 363, 14 July 2016.*

publish high-level allocations for each of the Agencies: *"If it was just a question of saying rough percentages in any specific year, I don't think necessarily that has to be secret."*[206] We were encouraged by this and explored the matter further with the Agencies themselves. However, the Agencies have made strong arguments against such a move. For example, the Chief of SIS said: *"I don't want to give stuff to the enemy so… I want us not to give detail to those that oppose us that might help them do the maths and work out our relative dispositions and our relative strengths."*[207] Other Agency Heads and other witnesses echoed those sentiments: they were clear that revealing individual allocations would provide an indication of how the UK was targeting its intelligence resources against those who seek to harm the UK and this would give our enemies an advantage.

Clarity

193. The concept of a 'Single Intelligence Account' was introduced, in part, to clarify and simplify the mechanisms of funding the Agencies, both to increase transparency and to reduce bureaucracy. However, in practice, the Agencies still receive significant separate funding streams from outside the core Single Intelligence Account, which they bid for throughout the year. This includes funding from the National Cyber Security Programme, the National Offensive Cyber Programme, the Counter-Terrorism Capabilities Fund and the Conflict, Stability and Security Fund.

194. Whilst this funding is incorporated into the published Single Intelligence Account figures at the end of each year, the amounts allocated are not known at the beginning of the year, and are instead added through a series of 'in-year adjustments' notified to Parliament through Supplementary Estimates. Funding from these additional streams is not guaranteed to be received, as it has to be bid for. This creates potential difficulties for planning or managing longer-term projects.

195. The additional funding streams also make it very difficult to monitor the financial performance of the Agencies 'in-year' and to make meaningful comparisons between budgets in different financial years. It also creates additional bureaucracy, and we have raised concerns that the existence of multiple additional funding streams provides an unnecessary layer of complication for the Agencies themselves. GCHQ told us:

> *It's not ideal… It is much more complex to keep track of these multiple funding sources and do multiple reporting to them… each of those different funding streams have different reporting requirements, different demands, want things cut in slightly different ways, and when that money is being fused with some of GCHQ's own money, the disentangling of all of that puts quite a strong administrative burden on us.*[208]

U. The Agencies receive a significant proportion of their funding from sources other than the Single Intelligence Account. Many of those funding streams are for work on areas such as cyber security, offensive cyber programmes, counter-terrorism projects, and capability building with key partners overseas, which could well be considered 'core' business. We recommend that such funding is incorporated into the Single Intelligence Account. This will reduce complexity, provide greater certainty of funding, aid good financial management, and increase transparency for Parliament and the public.

---

[206] *Oral evidence – National Security Adviser, 13 October 2016.*
[207] *Oral evidence – SIS, 17 November 2016.*
[208] *Oral evidence – GCHQ, 8 December 2016.*

Efficiencies and Savings

196. The Agencies have provided us with information regarding their efficiency savings, against the targets set in the 2010, 2013 and 2015 Spending Reviews. The Agencies told us that this has been a collaborative process, and therefore they have tended to report the savings as such. We have been told that the substantial majority of the savings across this period are categorised as 'efficiencies' (i.e. increasing outputs and/or reducing costs) as opposed to cuts.[209]

197. Many of the 'efficiencies' reported to us do not appear to represent actual reductions in spending, but include the 'notional monetisation' of supposed benefits and other non-cashable savings. 'Collaborative working' savings is one example of this – i.e. where SIS does not have to invest in something because it is using a solution developed by MI5, the amount that SIS would have had to pay separately is recorded as a saving. This issue is not new. In its 2012–2013 Annual Report, the Committee wrote:

> *Although the Agencies appear to be making good progress against their internal savings targets, the NAO [National Audit Office] 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 determine which were 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.*
>
> *There does seem to be a question as to whether the claimed savings and efficiencies which 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 [tri-Agency] finance teams must work together to address the NAO's findings and provide the necessary levels of assurance.*[210]

198. In its formal response to our Report, the Government said: *"Building on the findings in the National Audit Office report, [the Agencies] continue to refine and strengthen their internal and cross-Agency processes for challenging, validating and reporting savings."*[211] We remain sceptical. This is a somewhat 'smoke and mirrors' approach to efficiencies which may have enabled the Agencies to claim savings and efficiencies in some cases without necessarily reducing budgets or increasing outputs, and allowed the Treasury to claim progress against achieving its targets for Government spending efficiency. Nonetheless, we recognise that this is a matter of policy not confined to the Agencies, or indeed of their making given that they are operating within wider Government policies and frameworks. In that respect, it may be appropriate for the

---

[209] *There is one element of the 2015 Spending Round target, entitled "Foregone Investment", which is not a pure efficiency but instead represents the reprioritisation of core budgets to new capabilities. This represents £230m of the £1.3bn pan-Agency savings target.*

[210] ISC Annual Report 2012–2013*, HC 547.*

[211] Government Response to the ISC's Annual Report 2012–2013*, Cm 8736.*

Treasury Select Committee or Public Accounts Committee to consider this matter in the round.

199. With that said, for the coming period this issue is crucial since half of the additional £2.6bn of investment in the Agencies between 2015/16 and 2020/21 is due to come from 'efficiencies' – a significant figure of £1.3bn over five years. As a result, failing to deliver 'real cash' efficiencies will have a real impact on the capabilities of the Agencies. MI5 told us that *"all of that saving is part of our investment plan for the next five years, if the efficiency does not show up, the place where it doesn't show up is in our own plans for investment"*.[212] GCHQ agreed, noting that *"it is absolutely critical to the future that we do get those efficiencies. Otherwise we won't be able to fund things, so we will have to stop doing things."*[213]

200. MI5 commented that, at around 11% of the Agencies' budget settlement, the efficiency target *"is definitely stretching"*.[214] With this in mind, we asked the Agencies to outline their plans for delivering the required £1.3bn of savings. Each of the Agencies reported that they were currently on track with their efficiency plans, but also told us that they did not yet know where many of the later savings would be coming from, despite this representing the lion's share of the £1.3bn:

> *The biggest single component of the efficiencies plans for the next four and half years is the *** technology programme, which… has a very ambitious target to deliver £*** million worth of savings over the next five years and, candidly, we don't yet know where the last proportion of that will come from.*[215]

GCHQ told us that:

> *Some of it we haven't completely yet worked out to you how to do, to be honest. We have a programme. We have committed to do it. We think it's achievable. But for three years out we are not absolutely sure. We have committed to ***. It's a massively complex piece of work. It's going well to date, but we haven't made the really big decisions yet about how we do it.*[216]

201. Given the track record of the Agencies in generating verifiable and auditable cashable savings, it is concerning that such a significant proportion of much-needed investment is currently dependent on, as yet, unidentified savings.

V. In recent Spending Reviews there has been a tendency to claim savings benefits and efficiencies against rather intangible concepts, or by abandoning future projects that may have only been aspirational. This has led us to question the validity of claimed savings. There is no doubt that the savings required within the current Spending Review period are very substantial and without their successful delivery a number of critical investment projects will need to be cancelled. One year into the Spending Review period, some progress is being made, but there is still no plan for the total savings required over the whole period. When we return to this subject next year it is imperative that the Agencies have a full plan for the delivery of the full savings required. We will invite the National Audit Office to work with us next year to analyse the savings programme in greater detail.

---

[212] *Oral evidence – MI5, 1 December 2016.*
[213] *Oral evidence – GCHQ, 8 December 2016.*
[214] *Oral evidence – MI5, 1 December 2016.*
[215] *Oral evidence – MI5, 1 December 2016.*
[216] *Oral evidence – GCHQ, 8 December 2016.*

Staff Counsellor and Whistleblowing

202. A theme we have explored with all the Agencies this year is staff welfare and whistleblowing. GCHQ noted that it had a number of arrangements in place for staff: *"due to the nature of our work, it is imperative that staff feel able to use the relevant procedures and process. For that reason, a number of additional sources of support are available to staff. These include: an Employee Assistance team; a Staff Counsellor; and an Ethics Counsellor."*[217]

203. All three Agencies have had a Staff Counsellor since 1987, who is *"available to be consulted by any member of the Agencies regarding matters of conscience about the work of their service, or a personal grievance or other problem which has not been resolved internally"*.[218] The current Staff Counsellor is Julian Miller, a former deputy National Security Adviser. It should be noted that consultations with the Staff Counsellor are confidential and staff members' own line management chain and organisation will not be aware of the details of any case.

204. More recently, the Agencies have each established Ethics Counsellors who provide a route to discuss moral, ethical or other concerns, without the need to follow what could be seen as a more formalised process involving the Staff Counsellor. MI5 has led the way, establishing its Ethics Counsellor in 2006. SIS and GCHQ have now followed suit, appointing their own Ethics Counsellors in September 2012 and January 2014 respectively.

205. In order to get a sense of scale, the Committee asked how many staff have sought advice or guidance from the Ethics and Staff Counsellors:

- GCHQ told us that, since his appointment in January 2014, 128 staff had consulted its Ethics Counsellor (approximately five per month)[219] and that in 2015/16 there were six cases involving GCHQ staff who had gone to the Staff Counsellor.
- MI5 explained that its Ethics Counsellor sees approximately 40–50 staff per year and that one of its officers had consulted the Staff Counsellor in 2015, but none in 2016.
- SIS explained that its Ethics Counsellor was continually engaging teams across the organisation and proactively holding seminars and discussions on a range of issues that may pose moral and ethical questions. However, between September 2015 and July 2016, the Ethics Counsellor had been consulted by individual officers on 39 occasions. SIS believed that its officers consult the Staff Counsellor fewer than ten times per year on average.

206. The concept of whistleblowing is gaining increasing prominence across the public service as a whole, with 'Whistleblowing Awareness Week' having taken place in October 2016. MI5 explained that it was confident that it had sufficient whistleblowing procedures, including the ability for staff to contact the ISC should they consider a matter sufficiently serious. The then Director of GCHQ, Robert Hannigan, told us:

> *We have all sorts of routes that you can use to whistleblow, and we actively encourage people, if they've got concerns, to use one of them. So the Ethics*

[217] *Oral evidence – GCHQ, 8 December 2016.*
[218] *Statement by the Prime Minister to Parliament, 21 April 2016.*
[219] *Oral evidence – GCHQ, 8 December 2016*

Counsellor… he has direct access to me whenever he wants it. We have the [tri-Agency] Staff Counsellor, who is another route people can use outside GCHQ…

There are all sorts of routes people can come to, including the ISC if they feel all the other routes are either exhausted or not adequate, without breaching secrecy. Our staff survey results are pretty encouraging on this in that, first of all, the overwhelming majority of staff know these routes exist… [and] are confident that it wouldn't impact on their career, if they went to [them], which is encouraging.

So I think all the indications are good, that people, first of all, know they should raise a flag if they're worried about something, and they do, and, secondly, that it won't affect their career and they won't be somehow penalised. So there are lots of routes short of going and breaching official secrecy.[220]

207. SIS explained that it had similar procedures and the Committee asked whether any officers had formally made use of them in the last year (2015/16):

We had none reported that used the policy. So you are probably aware, we have a Reporting Concerns and Suspicions Policy – we don't come under the legislation in quite the same way but we apply, in essence, exactly the same principles and we… make it well known that that process exists. We ensure that our line managers are fully aware of that and it is… displayed and advertised.[221]

208. We note that all three Agencies have mentioned the ISC as an approved route by which staff can raise concerns whilst respecting the rules on the secrecy of their work and agree that this is sensible (although we also note that the Committee had not previously been informed that that was the case).

W. We are reassured that staff of all three Agencies have a number of routes to discuss moral, ethical, policy, legal or any other concerns, and that these appear to be reasonably well utilised. We were also interested to hear from Agency Heads that staff have been told that the ISC is an approved route for whistleblowing whilst protecting the secrecy of their work. We fully support this, but note that if the Agencies intend it to be used then the current bar on Agency staff being able to communicate with the Committee directly via secure email will need to be removed.

[220] *Oral evidence – GCHQ, 8 December 2016.*
[221] *Oral evidence – SIS, 17 November 2016.*

Contractors

209. The Committee has for a number of years questioned the Agencies on their use of contractors and consultants. When the Committee last investigated this matter in detail, in 2011, we found that the Agencies spent £400m per year on contractors and consultants. At the time this represented approximately 20% of the Single Intelligence Account and the Committee expressed concern that such a high level of spend may not ensure value for money in the long term.

210. However, reliance on outside contractors has continued to grow. The Agencies' total contract spend in 2015/16 was £1,223m, made up of £***m from GCHQ, £***m from MI5 and £***m from SIS. Together, this represents over one-third of the entire Single Intelligence Account in 2015/16.

211. This year we have explored all major contract spend in the Agencies. We have found that the majority of major contracts were for the delivery of specialised IT services, specific programmes, major engineering or infrastructure works, or facilities management (delivered by the likes of ***). Such contracts comprise both the supply of goods and/or discrete services, as well as the provision of associated staff.[222] The Agencies inform us that it is not possible to disaggregate the two elements, so we are unable to establish the amount spent specifically on staff supplied via these contracts.

212. However, one area where it has been possible to identify such spending is a single framework contract with *** known as ***. This is one of the largest categories of expenditure across the three Agencies. We have been told that this framework contract is a managed service that *"consolidates the supply of Professional Services from a range of agencies and independent contractors through a single point of entry to the market"*.[223] In our view it therefore represents additional staff.

213. These 'additional staff' cost significant sums of money:

- MI5 has reported that the majority of its time-hire contractor workforce, 470 personnel, were provided via this contract at a cost of £63m in 2015/16 (an average of £134,000 per person).
- GCHQ has obtained 494 contractors via this contract at a cost of £71m in 2015/16 (an average of £144,000 per person).[224]
- SIS has 279 contractors via this contract at a cost of £40m (an average of £143,000 per person).

Taken together, the three Agencies are engaging over 1,000 contractors via this framework contract at a very significant premium – over twice the cost of a permanent employee. In our view, the large number of these contractors also renders the Agencies' stated staff numbers somewhat misleading, given that this hidden off-payroll workforce amounts to around 10% of their official employee numbers.

214. Whilst we accept that some of these contractors may be carrying out highly technical roles requiring specialised and scarce skills (and in those circumstances a

---

[222] *For example, a contract to provide a new desktop IT system could include both the provision of new computer hardware, as well as staff to install the new system and provide long-term technical support for it.*
[223] *Written evidence – MI5, 18 July 2016.*
[224] *Written evidence – GCHQ, 18 July 2016.*

premium may be appropriate), not all are filling specialist roles, and in these cases it is difficult to see how the additional cost can be justified.

215. The Agencies have told us that it is appropriate to maintain a certain proportion of staff as contractors, since it is not always cost-effective to maintain or develop specialist skills in house. They have also said that maintaining a contractor workforce of this size provides greater flexibility, which is better suited to the ebbs and flows of major projects than a permanent staff. Nevertheless, the Agencies did accept that they need to do more to control spending in this area. MI5 has told us that it has *"initiated a more strategic approach"* to the way in which it uses contractors and consultants and that it is *"working through new governance, explicitly set up to reduce [its] use of time hire contractors"*.[225] Two initiatives set up to deliver on this aim are:

i) *"a 'decontractorisation' project to establish new posts, to be filled by permanent staff, undertaking work currently fulfilled by time hire contractors. This project forecasts the delivery of £***m savings by the end of 2020/21"*; and

ii) an internal development programme which, over the five-year SDSR period, will see 100 posts allocated to training programmes designed to enhance the skills of permanent employees in areas where contractors are currently used.[226]

X. Whilst we accept that there will remain a need, on occasion, to buy in specialist skills from outside, we nevertheless welcome initiatives to reduce reliance on time-hire contractors in circumstances where permanent staff are a more suitable and cost-effective option. Given the considerable growth in the number of time-hire contractors, and the costs involved, we recommend the National Security Adviser, as Principal Accounting Officer for the Single Intelligence Account, reviews use of permanent staff versus time-hire contractors focusing on the skills required, flexibility needed and costs involved (including the feasibility and value of delivering services in house).

216. We have also been concerned that, as the Agencies enter periods of considerable growth, where they lack in-house skills they may re-employ former staff as contractors to carry out work very similar to their previous duties. We therefore asked each of the Agencies to provide details of the numbers of former staff now working as time-hire contractors. GCHQ has approximately 200 such staff, SIS has 73 and MI5 has seven. These numbers offer very poor value for money and highlight a lack of adequate skills planning. Whilst it may always be necessary to re-hire some former staff in exceptional circumstances, this should be kept to a minimum given the potentially significant costs involved.

[225] *Written evidence – MI5, 18 July 2016.*
[226] *Written evidence – MI5, 18 July 2016.*

MI5 (Security Service)

Expenditure in 2015/16 [227]

Total expenditure

(£m)	Resource spending	Capital spending	TOTAL
2014/15	***	***	***
2015/16	***	***	***

Expenditure by category

- Staff costs: £***m
- Other revenue costs:
  - £***m (this includes professional services, accommodation charges, research and development, and IT systems)
  - £***m (non-cash items)
- Capital costs: £***m
- Against this, MI5 received income of £***m

Administration

Staff numbers[228]

	Total staff [229]	SCS [230]	Non-SCS
31 March 2016	4,053	46.5	3,870
31 March 2015	3,874	49.5	3,652

Recruitment in 2015/16

- MI5 recruited 427 staff, against a target of 402.
- This compares with 349 staff recruited in the 2014/15 financial year.

Staff diversity

At 31 March 2016	SCS	Non-SCS
Female staff	25%	41.9%
BAME[231] staff	0%	8.2%

[227] *As reported to the Committee in MI5's end-year report for the 2015/16 financial year.*
[228] *These figures refer to MI5's 'full-time equivalent' headcount.*
[229] *As noted in paragraphs 209–216, MI5 also engages a substantial number of additional staff via contracts.*
[230] *Senior Civil Service.*
[231] *Black, Asian and Minority Ethnic. Not all staff have declared their ethnicity; percentages refer to those who have declared it.*

Major projects in 2015/16	• The ALFA[232] programme, to improve the exploitation and retrieval of MI5's information (in progress) • Project BRAVO, to improve the efficiency of the use of the office space in Thames House (in progress) • Project CHARLIE, to modernise some of MI5's surveillance capabilities (***) – in progress
Policy	
Allocation of effort at 31 March 2016[233]	• International Counter-Terrorism: 64% • Northern Ireland-related terrorism: 18% • Hostile State Activity and Protective Security: 18%

Budget

217. MI5's spending has increased from £***m in 2014/15 to £***m in 2015/16 (an increase of almost 6%). We asked MI5 to explain why, in a period of otherwise heavily constrained public spending, it had been awarded a generous settlement, and for details of the additional outputs that had been delivered as a result. MI5 told us that the increase in budget was necessary to respond to the growing threat from international terrorism and technological developments that had made their work increasingly complicated:

> *In the period we are talking about the things that particularly drove it were of course the follow-on events from the so-called Arab Spring and the rise of what we now call Daesh, in particular in Syria, but in nine other countries today, along with the technology challenges we have had from shift to default encryption and multiplicity of apps that provide secure comms, and so on.*[234]

218. MI5 told the Committee that the extra resources had enabled it to disrupt 13 terrorist attacks against the UK in the three years to March 2017, which MI5 described as *"a pace we have just never experienced before"*.[235] MI5's work in this area is discussed in more detail in Section 3 (International Counter-Terrorism).

219. In addition to the funding received through the SIA, MI5 received separate funding from the National Cyber Security Programme (£***m), predominantly to support the cyber work which has now transferred to the new National Cyber Security Centre (NCSC).

220. MI5's budget was predominantly spent on staffing (***%), other operational costs (***%), IT (***%), research and development (***%), professional services (***%), and other administrative costs (***%). The main changes from 2014/15 spend were increases in staff costs, other operational costs, and research and development.

---

[232] *Where the codenames of programmes and projects have required redaction, these have been replaced by the NATO phonetic alphabet for ease of reading. The original codenames can be found in Annex A.*
[233] *The 'allocation of effort' relates to the proportion of MI5's operational and investigative resources by spend.*
[234] *Oral evidence – MI5, 1 December 2016.*
[235] *Oral evidence – MI5, 1 December 2016.*

Staffing

221. The number of staff working at MI5 increased by approximately 5% between March 2015 and March 2016. MI5 reported that it had exceeded its recruitment target for 2015/16, recruiting 427 staff against a target of 402. MI5 told us that it expects to have 4,950 staff by March 2020: this represents an increase of 22% in just four years.

222. It takes a significant amount of time and effort to train intelligence officers to a level that they are producing useful outputs. MI5 told us that *"typically a new intelligence officer takes about two years to come through their Intelligence Officer Development Programme, during which period they will… be employed into different kinds of roles"*.[236] We therefore asked MI5 to explain how it planned to absorb such a large number of new staff into its workforce at a time of high threat. MI5 acknowledged that *"through a phase of growth, it is unavoidable that average experience levels will actually decline, which feels perverse in a period of high threat"*. However, MI5 was keen to emphasise that it could cope with this risk by ensuring that postings to *"frontline business areas"* were managed to ensure the correct balance of experienced and new officers was maintained. We were assured that MI5 had *"quite a lot of experience of spreading that load and managing the absorption across the whole of the business"*.[237]

223. In 2015/16, MI5 spent £***m (52% of its overall budget) on contracts. This was broadly split into three categories: managed services contracts (e.g. facilities management), managed delivery contracts (e.g. the installation of a new IT system), and time-hire contractors who *"provide on a more granular, tactical, flexible basis the skills that we don't have in the permanent workforce to help us make the most of all of that spend; so things like business architects, things like specialist IT skills which we don't have enduringly in the organisation, although we are trying to change that in some cases"*.[238]

224. We questioned such a high level of spend. MI5 told us that it is actively seeking to reduce its reliance on contractors where it makes more sense to bring the skills in house:

> *Over the [next] four and a half years…we have a programmatic approach to what we call the decontractorisation, where we expect to make £*** million of savings by continuing to do exactly what you say [bring more skills in house]*.[239]

Spending on agents

225. Agents provide information to the Agencies, and sometimes undertake tasks on their behalf.[240] They are not employees of the Agencies. They would typically be people who are close to people or organisations of intelligence interest, such as terrorist groups or hostile foreign governments. Most are paid (albeit that money may not be their primary motivation for assisting), some may continue to receive payments after they 'retire', and agents whose safety is in danger will sometimes be relocated and given new identities. In the past, the Agencies have emphasised to the Committee how seriously they take their ongoing duty of care towards their agents. In 2015/16, MI5 spent £***m on agent costs.

---

[236] *Oral evidence – MI5, 1 December 2016.*
[237] *Oral evidence – MI5, 1 December 2016.*
[238] *Oral evidence – MI5, 1 December 2016.*
[239] *Oral evidence – MI5, 1 December 2016.*
[240] *Formally defined as a Covert Human Intelligence Source (CHIS) under the Regulation of Investigatory Powers Act 2000.*

226. The use of agents clearly has scope to be highly controversial: the Agencies are handing significant amounts of money to people who may have close links to terrorism or serious crime, or who may work for foreign governments. Furthermore, the agents and the information provided by them are not necessarily reliable: in 2015 it was reported in the media that an MI5 agent was allegedly recruited by a terrorist in Syria and sent back to Britain to launch an attack. Nevertheless, agents are critical to MI5's work. In December 2016, MI5 told us:

> *I don't want to talk about agents without acknowledging the fact they take risks for us, they do brave things for us, they are the intelligence collection asset that we could not operate without. They give you insight that technical intelligence cannot give ***.*
>
> *Often we will say to ourselves in [internal] meetings about our investment, ***. We cannot do everything that way of course, otherwise we would.*[241]

Major projects

227. We have considered three of MI5's major projects for 2015/16. These are detailed below.

228. The ALFA programme (£***m over eight years) is intended to improve the exploitation and retrieval of MI5's information. We were informed that there are currently a myriad of legacy IT and information management systems within MI5 that need to be updated and joined up more effectively. Part of the programme will help to address this.

229. The programme has experienced significant problems since it began in 2014/15. The original scope of the programme has had to be reduced, the forecast spend has increased by 10% (albeit still inside the Treasury-approved cost envelope) and it is taking longer than first thought to deliver. In March 2016, the Major Projects Authority (MPA) reviewed the programme and gave it a delivery confidence assessment of AMBER/RED. The MPA made six recommendations, which have now been completed. A further MPA review, completed in July 2016, improved the rating to AMBER, recognising the action that had been undertaken. The Director General of MI5 also commissioned two independent external reviews of the programme, which have helped to drive further improvements.

Y. The Agencies' primary business is information: everything they do is underpinned by their ability to record, maintain and use that information properly. The ALFA programme is crucial to MI5's core business of managing information. The programme has faced major problems since its inception and there remain significant risks to its successful delivery, despite some positive efforts from MI5 over the last year. It is essential that this programme, and other information management programmes being put in place across the UK intelligence community, succeed.

230. Project BRAVO (£***m over five years) will increase MI5's accommodation space and enable efficiency savings through more effective use and release of existing estate. The project should result in around 400 extra desks in MI5's Headquarters by 2017/18. The project is moving into its final delivery phases and has been given a GREEN rating from the MPA. Greater than expected efficiencies have been achieved through the

[241] *Oral evidence – MI5, 1 December 2016.*

re-use of IT equipment from the closure of one of the London offices and the forecast total spend on the project is now estimated at £***m.

231. Project CHARLIE (£***m over five years) is intended to modernise some of MI5's surveillance capabilities ***. The project has been given an AMBER rating following concerns about the principal supplier. ***.

Allocation of effort

232. MI5 staff are allocated across three broad categories, *Operational, Capability* and *Corporate services*:

- Operational work involves running investigations and operations to disrupt threats. MI5 told us that in 2015/16 International Counter-Terrorism accounted for around 64% of its operational and investigative resource by spend, with Northern Ireland-related terrorism accounting for around 18% and Hostile State Activity and Protective Security accounting for the remaining 18%. The allocation of effort was broadly the same in 2014/15.
- Capability roles provide a range of support to MI5's operations, including surveillance, the development of technical capabilities, and analysis.
- Corporate services includes: legal, security, HR, finance and strategy, facilities, and information management.

Secret Intelligence Service (SIS)

Expenditure in 2015/16 [242]

Total expenditure

£m	Resource spending	Capital spending	TOTAL
2014/15	***	***	***
2015/16	***	***	***

Expenditure by category

- Staff costs: £***m
- Other administration costs: £***m
- Operational expenditure: £***m
- Other programme costs: £***m
- Capital costs: £***m
- Non-cash items: £***m

Administration

Staff numbers[243]

	Total staff [244]	SCS	Non-SCS
31 March 2016	2,594	74	2,520
31 March 2015	2,479	75	2,404

Recruitment in 2015/16

- SIS recruited 98% of its target number of staff in 2015/16 (*** against a target of ***).
- This compares with 236 staff recruited in the 2014/15 financial year.

Staff diversity

At 31 March 2016	SCS	Non-SCS
Female staff	24.1%	37.8%
BAME[245] staff	0.0%	6.8%

[242] *As reported to the Committee in SIS's end-year report for the 2015/16 financial year. Includes Annually Managed Expenditure (AME).*
[243] *These figures refer to SIS's 'full-time equivalent' headcount.*
[244] *As noted in paragraphs 209–216, SIS also engages a substantial number of additional staff via contracts.*
[245] *Not all staff have declared their ethnicity; percentages refer to those who have declared it.*

Major projects in 2015/16	• DELTA, which aims to increase the capacity of SIS's London estate • ECHO, which is a new information management system • Cross-Served Desktop Global, which would bring the same SIS computer desktop to all its locations globally
Policy	
Allocation of effort at 31 March 2016	• Operational: 39%, of whom: o approximately half work on geographical areas o approximately a third work on counter-terrorism o less than a quarter work on thematic issues • Operational support (including global network enabling, covert operations, data exploitation, operational security, and operational technology): 22% • Corporate services (including legal and private offices; human resources; finance, estates & business change; IT infrastructure; security and compliance; science, research and innovation; and policy, requirements and communications): 39%

Budget

233. SIS was allocated a budget of £***m from the SIA in 2015/16. However, SIS also received significant additional sums (an extra 19%) from seven separate additional funding streams that year, resulting in its total spending being £***m. This can be compared with total spending of £***m in 2010/11 – an increase of 25% across five years of otherwise heavily constrained public spending.

234. SIS has informed us that its budget allocation from the SIA is projected to increase to £***m (an uplift of 28%) over the four years to 2019/20 (noting that it is unable to predict allocations of budget from separate additional funding streams as these are usually allocated annually). When we questioned these large increases, SIS responded:

> *I did conclude… that we were too small, we were sub scale. We did that absolutely in the knowledge that this country is not flush with cash and that we are in an austerity environment but I did feel it was my duty to say that and it was that that underpinned the conversation that we had in the SDSR which has resulted in the uplift… the scale of the ask, the increasing, the need for presence, and the fact that the amount of enabling effort that we require to do things that would have been cheaper beforehand has significantly gone up. Put those together, understanding that we can do a great deal through joint working and efficiency, but you still get an objective need to make our capability bigger.*[246]

[246] *Oral evidence – SIS, 17 November 2016.*

235. We also asked SIS whether it was in a position to spend this additional funding effectively, given how sharp the increase in funding is. In response, SIS said:

> *A big part of this is recruitment and headcount, and if you tracked our capacity to grow at the speed that the uplift we have been given implies, then we are on target. We have been doing this for a few years and we have hit those targets consistently. Of course I am very very focused on this and we pushed the machine very hard and bringing people into the service is a complicated business at the best of times.*[247]

Staffing

236. SIS has made it clear that most of its additional budget will be spent on increasing its headcount. From a recent low of 2,368 full-time equivalent staff at March 2014, SIS plans to increase to 3,231 staff by March 2020 – a 36% increase in headcount over six years. Questioned on whether it would be possible to bring in so many new staff so quickly, SIS said:

> *So we are very aware that it is a challenge. If I focus on the absorption as opposed to the recruitment for the moment, a lot of the investment that we have been doing this year is in the things that will enable that, recruitment included, and up powering our learning and development effort, and we are looking really hard at what sort of people we bring in and where we are going to put them and then making sure they are going to be alongside people who are more experienced.*[248]

237. In a public speech given in Washington DC in September 2016, 'C' said that *"the information revolution fundamentally changes our operating environment"*, implying that a large proportion of the new staff might be allocated to cyber-related work. SIS said:

> *[One weighting in our workforce plan] is towards more highly skilled technologists. This is not to say we lose our soul as fundamentally a people organisation that is about relationships, but we need more skilled people who can work at the higher end, particularly, of data, science and operational technology. So for instance we have just taken the decision to significantly increase earlier the number of people that we put into what will be a joint cadre between the three services where we recruit and trade and then deploy our data analytic.*[249]

238. This Committee previously criticised an expensive redundancy exercise run by SIS in 2011/12, when it made payments to 111 staff to take early retirement.[250] Given that a few years later it is looking to increase staff numbers by considerably more than this, it does not appear to have been well planned. When asked, 'C' declined to justify it, instead simply saying:

> *I make it a rule not to comment on decisions made by my predecessors… I was not in the leadership then… It was an extraordinary time, do you remember? It was just after the banking crisis and all of that.*[251]

239. We also asked SIS about its policy regarding re-engagement of former employees as contractors. At March 2016, there were 73 people who had been re-engaged in this

---

[247] *Oral evidence – SIS, 17 November 2016.*
[248] *Oral evidence – SIS, 17 November 2016.*
[249] *Oral evidence – SIS, 17 November 2016.*
[250] *Once the departure of staff other than through redundancy is included as well, SIS's headcount reduced by a total of 200 staff in 2011/12.*
[251] *Oral evidence – SIS, 17 November 2016.*

manner, with the average interval between leaving and re-joining as a contractor being 33 months. On this subject, SIS said:

> *SIS policy is that it does not engage former members of staff as contractors. Exceptionally, when a hiring manager considers that there is no alternative other than to engage an ex-employee for a contractor role, the proposal may be considered.*[252]

We note that three of the 73 re-employed staff had taken redundancy payments from SIS.

Spending on agents

240. SIS has informed us that it spent £***m on agent fees in 2015/16, and £***m on operational and agent expenses (the former consists of payments to agents for services rendered, and the latter consists of other expenses incurred by – and in running – agents). Given that SIS's primary intelligence-collecting role is running agents, it is unsurprising that a significant proportion of its non-staff costs are related to this. In terms of agent fees, SIS has informed us that *"the amounts that agents receive will range from hundreds of thousands of pounds to zero"*, with the highest single amount paid to an agent in 2015/16 being £***.[253] However, SIS has pointed out that the benefits provided by agents' intelligence can be very substantial, meaning even large agent-related costs can represent good value for money. 'C' explained that whilst it can be a lot of money it must be looked at *"in the context of the countervailing benefit"*. He noted that certain operations, which are based on agents, allow the Government to make significant savings elsewhere (for example, ***).[254]

241. It is not only current agents who are paid by SIS:

> *There are *** retired agents that are still being paid. The average amount is £*** per annum.*[255]

Additionally, where agents are at risk of being uncovered, they sometimes need to be resettled by SIS (whether in the UK or elsewhere) *"which is a significant and expensive undertaking"*; SIS informed us that its resettlement team has looked after *** cases during the last five years.[256]

Organisational Design Review

242. SIS has informed us that, from December 2015 to June 2016, it *"engaged with a team of consultants to review our current structures and ways of working, and to produce recommendations for improvements"* as part of its Organisational Design Review. The main result of this review appears to have been a major restructuring of SIS's Directorate-General for Operations. This Directorate-General had hitherto been split into three geographic regions and three themes.[257]

243. SIS informed us that, from mid-September 2016, these Directorates were abolished – and the Directorate-General has instead been based around the intelligence

---

[252] *Written evidence – SIS, 5 January 2017.*
[253] *Oral evidence – SIS, 17 November 2016.*
[254] *Oral evidence – SIS, 17 November 2016.*
[255] *Written evidence – SIS, 5 January 2017.*
[256] *Oral evidence – SIS, 17 November 2016.*
[257] *These were: ***; Cyber and ***; Counter Proliferation ***; Counter-Terrorism; ***; and ***.*

community's three strategic themes (as outlined in the Security and Intelligence Agencies' Plan) of:

- Strategic Advantage (which aims to provide targeted intelligence to the UK, *** and managing threats to the UK from hostile foreign states);
- Counter-Terrorism; and
- Cyber and ***.[258]

244. Director-level management now consists of four Theme Directors who *"will own all operational resource across the three themes"*. Operations will then be conducted *"by Missions with staff from across the three themes"*.[259] Given that there are only three themes, we asked SIS what the fourth director would work on, to which it replied:

> *** *[which] is as much a theme as a place, frankly… The importance of the high-level contacts and relationships we have there… need… to be considered at the strategic level… I did need strong geographic focus at that level when it came to the Middle East.*[260]

245. SIS says that this reform was aimed at ensuring that SIS can respond in a more agile manner to swiftly changing priorities, as opposed to having staff stove-piped into geographical areas. We asked SIS whether the split of areas was fair given that, across the intelligence community, it is only the natural leader on the Strategic Advantage theme (with MI5, for example, leading on terrorism). On this, SIS said:

> *I bridle at the idea of any of us owning one of these themes. The reason we were successful in the SDSR is we convinced the Government that we were intent on blending our capabilities against these three priorities. So if there were to be a huge uplift on [Counter-Terrorism], I would not conclude that that was a problem for SIS and good for MI5. We have completely integrated capabilities.*[261]

246. We also explored what this restructuring means operationally. The previous arrangement of the Directorate-General was largely geographical or workstream based; there is clearly a risk that 'deep' subject matter or regional expertise may be unintentionally dissipated by these reforms. On this, SIS said:

> *When I was the Director for Counter-Terrorism, I was… commanding… the terrorist stuff and then I had a colleague who was the Director for [a region] and he was commanding a load of [geographic] stuff, but terrorism happens [there too], and we were distantly sort of fiddling about with the boundary and trying to work out who does what. And I think what I really like about this innovation is we have just abandoned that now. There is a team that is arranged geographically that works for both the Director for Counter-Terrorism and the Director for [the region]. That means the [regional] and terrorism Directors have themselves to work together to work out what the most important and useful lines of operation can be. So it is a significant improvement on flexibility. It gets more out of our capabilities, but it*

---

[258] *Whilst two of these themes share the name of predecessor Directorates, we understand that they will be organised and managed very differently.*
[259] *Oral evidence – SIS, 17 November 2016.*
[260] *Oral evidence – SIS, 17 November 2016.*
[261] *Oral evidence – SIS, 17 November 2016.*

does put a premium on the Directors in particular working in a collegiate way, in a way that perhaps they have not always done in the past.[262]

247. We note that SIS employed consultants on this review, at a cost of £798,000. We asked SIS whether it really needed to employ external contractors (at such a high cost) in order to tell it how to organise itself:

I believe that they were, because I would be haunted if we reinvented the wheel, if we merrily, in a culture of exceptionalism, barrelled down the track saying "We are going to do it like this", and ignored the fact there is an enormous amount of thought and expertise in the private sector and elsewhere.[263]

Major projects

248. Over the last year we have looked at two major SIS projects, as detailed below.

249. DELTA is aimed at increasing SIS's London accommodation through the refurbishment of Vauxhall Cross (including the introduction of hot-desking) and renting space in a building in London belonging to another Government Department (***) – where SIS will co-locate some administrative teams ***. It has a whole-life cost of £***m from April 2014 to March 2025. SIS has informed us that approximately half of this sum will be spent on rent in the other building, with the remainder being spent on the refurbishment of both the space in the other building and Vauxhall Cross.

250. We note that the Agencies are, between them, currently in the process of disposing of five buildings in central London. Any one of these could potentially have been used in place of renting new space in the other building. Additionally, the other building is subject to ***; which, in June 2016, contributed to SIS identifying a 'red risk' that *"costs are higher than anticipated"*. SIS told us that it was working hard with the supplier and other parties involved to get greater clarity about the commercial arrangements, and was seeking a reduction in price:

We have been working very hard… basically to get (a) clarity and (b) reductions. We are not, as we wouldn't be at this stage, completely there but we have (a) more confidence and (b) we have already reduced the costs somewhat of our going into [the other building].[264]

251. We questioned the logic of choosing the other building in preference to using an existing redundant building from the Agencies' central London estate. SIS explained that there are operational reasons for wanting to be in the same building:

*I am extremely focused on the extent to which we can create a mutually reinforcing dynamic between intelligence, security ***… so I think the fact of being in [the other building] offers us significant advantages…*[265]

This explanation can only make sense if it is primarily some of SIS's *** teams that move into the other building. However, evidence provided to the Committee in July 2016 only specifically mentioned SIS's administrative teams moving into the building (and this reflects the May 2016 Outline Business Case). We note that by the time of the Final

[262] *Oral evidence – SIS, 17 November 2016.*
[263] *Oral evidence – SIS, 17 November 2016.*
[264] *Oral evidence – SIS, 17 November 2016.*
[265] *Oral evidence – SIS, 17 November 2016.*

Business Case in November 2016 there was reference to *** teams; however, the late inclusion suggests that this was not the driving force behind the move. We will be scrutinising this project further, with the assistance of the National Audit Office.

252. We have also looked at ECHO, which is a new information management system. It has a whole-life cost of £***m from April 2016 to March 2025. SIS states that this project is necessary due to the age of its existing systems, and to reduce risks concerning information and records – thus ensuring it can meet its disclosure obligations.

253. Given that this Committee has severely criticised SIS's record keeping in the past, we support efforts to improve this. When we asked SIS about its confidence in the new system's efficacy, we received a confident response:

> *So us being able to search across the entirety of everything that we have written or reported or ingested is vital. I think it will provide a significant powerful uplift. It also ensures that we can be compliant, particularly against the innovations in the [Investigatory Powers] Bill, but more broadly. So it is important… it is basically already there, it is working well. It involves some cultural changes of service, but it is cultural changes I want and we will turn off the old system at the end of [November 2016].*[266]

Allocation of effort

254. A total of 39% of SIS's staff work directly on operational matters. A further 22% work on operational support, which covers a wide range of direct assistance provided to operational teams including physical security, supporting deployed staff, technological support, communications, maintaining operational secrecy, enabling the military, data exploitation, and operational skills training.

255. The remaining 39% of SIS's workforce are employed in corporate services. Of these, the three biggest areas of work are:

- IT infrastructure (31% of corporate services staff);
- security and compliance (22% of corporate services staff); and
- finance, estates and business change (21% of corporate services staff).

[266] *Oral evidence – SIS, 17 November 2016.*

Government Communications Headquarters (GCHQ)

Expenditure in 2015/16[267]

Total expenditure

£m	Resource spending	Capital spending	TOTAL
2014/15	***	***	***
2015/16	***	***	***

Expenditure by category

- Programme costs: £***m
- Administration costs: £***m
- Capital costs: £***m
- Annually Managed Expenditure: £***m

Administration

Staff numbers[268]

	Total staff[269]	SCS	Non-SCS
31 March 2016	5,806	55	5,751
31 March 2015	5,564	49	5,515

Recruitment in 2015/16

- GCHQ recruited 500 staff, against a target of 640.
- This compares with 443 staff recruited in the 2014/15 financial year.

Staff diversity

At 31 March 2016	SCS	Non-SCS
Female staff	18%	35%
BAME[270] staff	2%	3%

[267] *As reported to the Committee in GCHQ's end-year report for the 2015/16 financial year (including AME).*
[268] *These figures refer to GCHQ's 'full-time equivalent' headcount.*
[269] *As noted in paragraphs 209–216, GCHQ also engages a substantial number of additional staff via contracts.*
[270] *Not all staff have declared their ethnicity; percentages refer to those who have declared it.*

Major projects in 2015/16	• The FOXTROT programme, an Equipment Interference programme to increase GCHQ's ability to operate in an environment of ubiquitous encryption (in progress) • Replacement Facilities Management Contract, to deliver a single facilities management solution for the whole of the GCHQ estate (excluding the private finance initiative at Benhall) (in progress) • The High-End Data Centre capability, involving the creation of a new high-end data centre (in progress)
Policy	
Allocation of effort at 31 March 2016	• Capability Exploitation:[271] 24% • Engineering: 19% • Specific geographical coverage to reflect the threats in Strategic Defence and Security Review 2015, which include the Middle East, South Asia and former Soviet Union: ***% • Other operational activities (including counter-terrorism, protective security, cyber defence, offensive cyber, economic security, weapons, and serious crime): ***% • Corporate services (including human resources, finance, legal, IT services, policy and compliance): 27%

Budget

256. GCHQ's budget has increased by almost 18% between 2014/15 and 2015/16, rising from £***m to £***m. GCHQ's budget is set to increase still further as part of the 2015 Spending Review settlement, which provided a 17% real terms increase for the Agencies.

257. We asked GCHQ to explain why such a generous settlement had been awarded, and the additional outputs that would be delivered as a result. GCHQ told us that the dramatic increase between 2014/15 and 2015/16 was *"directly linked to the revaluation on plant and machinery"* (accounting for approximately £100m of 'budget adjustments').[272] However, GCHQ acknowledged that, even allowing for this accounting adjustment, it had received a very significant budget increase with more to come. GCHQ explained that this was because it was being asked to deliver more, across a wider set of areas, and that technological developments are making its work increasingly more complicated:

> *We are being asked to do more, critically on cyber, on the National Cyber Security Centre, on offensive cyber outputs… we have had fantastic success on CT [and] on crime. All of that has been in quite new areas, demanding new technology and new approaches which have obviously meant new spending… we actually need to invest to stand still… Terrorism is a good example* ***.[273]

[271] *Capability Exploitation is charged with finding and exploiting both secret and open source information in support of the intelligence and security missions and ensuring that GCHQ remains at the cutting edge of tradecraft and technology.*
[272] *Written evidence – GCHQ, 18 July 2016.*
[273] *Oral evidence – GCHQ, 8 December 2016.*

258. Of GCHQ's total budget for 2015/16, a sizeable amount (***%) is derived from six separate funding streams which they bid for throughout the year. The two largest of these streams are the National Cyber Security Programme (£***m) and the National Offensive Cyber Programme (£***m).

Staffing

259. In order to meet the new demands, GCHQ will be increasing its headcount significantly. The number of staff working at GCHQ increased by approximately 4% (to 5,806) between March 2015 and March 2016; however, GCHQ told us that it expects this to increase by 14% over the next four years, bringing the total to 6,639 staff by March 2020.

260. Given that in 2015/16 GCHQ reported that it had a shortfall in recruitment of approximately 22% (recruiting 500 staff against a target of 640), we asked how this ambitious target would be achieved. GCHQ told us that the key obstacle to achieving its target in 2015/16 was a lack of security vetting capacity, which it was seeking to address:

> *We have surged a lot of people into vetting… we had 51 [vetting officers] in July this year [2016]. We will have 110 by next summer to work through this… It is having an impact. We will clear the backlogs by the end of next year.*[274]

261. Intense competition from the private sector for people with the skillsets GCHQ is seeking to recruit presents a further challenge. GCHQ acknowledges this as a significant issue, but is confident in the plans it has in place to address the situation. This was discussed in more detail earlier in this report, in Section 5 on Cyber Security.

262. We also questioned whether GCHQ would be able to absorb and leverage such a rapid increase in staff numbers. GCHQ told us:

> *Apprentices and other staff brought in at [a] young age on various different schemes which we run… are at the heart of the mission, and some of our most difficult operations are on the Internet within a couple of years of joining. So actually we are getting value from people very early on. The challenge will be retaining them obviously and developing them and giving them a sort of rounded career.*[275]

263. We also asked GCHQ about the extent to which it was re-employing former staff as contractors, as this appears to be on the increase throughout Government. GCHQ informed us that approximately 200 individuals who had previously been permanent employees were working for GCHQ via a contractor (as at January 2017). GCHQ has said that this is because of the scarcity of the specialist skills that GCHQ requires.

Major projects

264. We have considered two of GCHQ's major projects for 2015/16, detailed below.

265. GCHQ said that the FOXTROT Programme – costing £***m over five years) is in part a response to the growth of ubiquitous encryption ***.

---

[274] *Oral evidence – GCHQ, 8 December 2016.*
[275] *Oral evidence – GCHQ, 8 December 2016.*

266. However, since its establishment, the programme has suffered a number of delays. GCHQ told us that *"the task has become more complex, the skills shortage has become more apparent, ***"*.[276] This resulted in a one-year delay for the delivery of 'Tranche 1' capabilities (***), and an AMBER/RED rating[277] from the MPA. GCHQ told us:

> *I think it's one of those programmes that's red because it's really really difficult. So we would be surprised if it wasn't red. We discuss this at the Board regularly. It is our number one priority and our number one worry.*
>
> *I think we are doing all the right things. There are some problems that are just very, very hard to solve, not just because it's technically difficult, but because the skills aren't there.*[278]

267. It is concerning that a programme described as critical to GCHQ's work is marked AMBER/RED, and assessed as likely to remain this way. We urge GCHQ to reassess what more it can do to improve the outlook of this project and to ensure that its recruitment and skills management approach for the future addresses the skills shortage issue in this area.

268. Project GOLF (£***m over ten years) is a project to enhance the supercomputing capacity that supports much of GCHQ's work. GCHQ has told us that this project is particularly critical, as it predicts that *"projected mission needs will exceed existing data centre capacity limits in ***"*.[279] GCHQ noted that its relationship with the US brought significant benefits ***.[280] GCHQ has reported that this project *** is on track to be fully operational in early 2018.

Allocation of effort

269. Approximately 30% of GCHQ staff perform operational work, covering:

- specific geographical coverage to reflect the threats in the Strategic Defence and Security Review 2015, which include the Middle East, South Asia and former Soviet Union; and
- other operational activities (including counter-terrorism, protective security, cyber defence, offensive cyber, economic security, weapons and serious crime).

270. Almost half of GCHQ's staff work on developing and supporting GCHQ's technical capabilities:

- 24% on Capability Exploitation (finding and exploiting both secret and open source information in support of the intelligence and security missions and ensuring that GCHQ remains at the cutting edge of tradecraft and technology); and
- 19% on Engineering (building the systems required to support this activity).

---

[276] *Written evidence – GCHQ, 18 July 2016.*
[277] *Meaning that successful delivery is unachievable or in doubt unless action is taken.*
[278] *Oral evidence – GCHQ, 8 December 2016.*
[279] *Written evidence – GCHQ, 18 July 2016.*
[280] *Oral evidence – GCHQ, 8 December 2016.*

271. The remaining 27% work in corporate services (including human resources, finance, legal, IT services, policy and compliance).

272. GCHQ also provides support to military operations (SMO) (its allocation of effort to this area is not reported separately but is included within other categories). In recent years, this has focused on supporting UK operations in Iraq and Afghanistan. However, in the absence of a current major deployment of UK combat forces, GCHQ told us that the nature of this was changing:

> *Supporting the military has been a huge part of our history for a hundred years and continues to be. If anything, it's growing now actually, in a different way. I mean, it's massive in Afghanistan but that has changed and I think it's now more two way. ***. So the relationship is very broad and very deep.*[281]

Estates

273. GCHQ operates from a number of sites across the UK: this Committee has consistently criticised its inability to manage its estate. For example, when it built 'the Doughnut' in Benhall, Cheltenham in 2004 (at the time the largest building constructed for secret intelligence outside of the USA), it was already too small for the number of GCHQ staff. 'The Doughnut' continues to cause problems: despite improvements in the use of the existing space over the years, and the building of a new premises ('the Cube') in part of its car park, it operates at more than 125% of designed capacity on any given day.

274. In explaining why they found themselves in this situation (again), GCHQ told us:

> *Over recent years GCHQ has received additional funding for staff to work on counter-terrorism and to address the cyber challenge. While this staff growth has been accommodated within the MOB ['the Doughnut'] for cost efficiency, the building is now operating beyond its optimal capacity. Further growth to address the ISIL threat is scheduled. Moreover, intelligence tradecraft and ways of working have changed, resulting in a need for additional and different accommodation.*[282]

275. In the Spending Review, GCHQ sought – but failed – to secure extra funding for additional accommodation in the next five years. It has reported that *"GCHQ's estate will remain under significant pressure with this felt most keenly in Cheltenham"*.[283] As a result, it has cancelled its medium-term plan to acquire new estate in the Cheltenham area, and developed a new accommodation strategy. GCHQ informed us that this follows a decentralised business model, with locations *"selected to maximise access to diverse and talented people"*.[284] Decentralising will result in three hubs – Cheltenham, London and the North West – around GCHQ's existing estate, with particular expansion and growth aimed in the North West. GCHQ told us:

> *I think we do have a new strategy which meets indeed the Committee's criticisms of slightly haphazard approach in the past. It is coherent. It is increasingly tri-Agency. As you know, there is a vision for the three agencies.*
>
> *It's both meeting our immediate pressures. As you know, our biggest staff concern at the moment is lack of space in Cheltenham, one of the reasons why we built the*

[281] *Oral evidence – GCHQ, 19 January 2017.*
[282] *Written evidence – GCHQ, 30 August 2016.*
[283] *GCHQ Annual Accounts, 2015/16.*
[284] *Written evidence – GCHQ, 30 August 2016.*

Cube, so called, in the car park as a kind of immediate measure to bring us another 450 desks. But we recognise as a Board that actually that is a short-term measure. It's not the answer.

The answer for all sorts of reasons, including recruitment and diversity, is to push outside Cheltenham. Cheltenham, I think, will always be our centre of gravity, but in the future we need a number of different things.[285]

Z. The management of GCHQ's accommodation has long been an area of serious concern to this Committee. We note GCHQ's adoption of a new approach, which seeks to address not only its lack of physical space, but also its diversity issues, and will examine whether or not it provides a coherent solution in due course.

[285] *Oral evidence – GCHQ, 8 December 2016.*

Defence Intelligence (DI)

Expenditure in 2015/16[286]

Total budget and outturn

£m	Resource spending	Capital spending	TOTAL
2014/15	320.5	0.7	321.2
2015/16	303.6	11.9	315.5

Expenditure by category

- Operational costs:
  - Personnel costs: £211m
  - Equipment support: £61m
  - Research and development: £30m
- Administration costs:
  - Inventory/other consumption: £3m
  - Infrastructure: £9m
  - Other administrative costs: £15m
- Against these areas of expenditure, DI received an income of £25m

Administration

Staff numbers[287]

	Total staff	SCS and military equivalents	Non-SCS and military equivalents
31 March 2016	3,655	4/6	1,444/2,201
31 March 2015	3,697	6/8	1,359/2,324

Recruitment in 2015/16

- DI recruited 171 civilian staff in 2015/16.
- This compares with 212 civilian staff recruited in the 2014/15 financial year.[288]
- Other vacancies are filled by Armed Forces personnel posted from their respective Services.

[286] *As reported to the Committee in DI's end-year report for the 2015/16 financial year. Includes Annually Managed Expenditure (AME).*
[287] *These figures refer to DI's 'full-time equivalent' headcount.*
[288] *This figure includes both internal civil service and external recruitment.*

<table>
<tr><td>Staff diversity</td><td><table>
<tr><th>At 31 March 2016</th><th>SCS</th><th>Non-SCS</th></tr>
<tr><td>Female staff</td><td>0%</td><td>36%</td></tr>
<tr><td>BAME[289] staff</td><td>0%</td><td>5%</td></tr>
</table></td></tr>
<tr><td>Major projects in 2015/16</td><td>• PRIDE 2, which plans to integrate certain capabilities of No 1 Aeronautical Information and Documentation Unit and the Defence Geographic Centre into DI's RAF Wyton base, and removes DI's footprint at Feltham, Northolt and Hermitage
• PRIDE 'One DI', which relocated certain further DI capabilities, those of single Service intelligence units and representatives from allies and other parts of Government to RAF Wyton</td></tr>
<tr><td colspan="2">Policy</td></tr>
<tr><td>Allocation of effort at 31 March 2016</td><td>• Total Operational and Analysis: 80%, of which:
o All source analysis and assessment: 8%
o Collection and analysis, including Cyber: 72%
• Operational support: 15%, of which:
o Armed Forces' Security and Intelligence Training: 13%
o Armed Forces' Intelligence Policy and Future Capability: 2%
• Corporate services: 5%</td></tr>
</table>

Budget

276. DI spent £315.5m of its annual budget allocated by the Ministry of Defence in 2015/16, a slight reduction from 2014/15. However, in addition to this, it spent a further £***m provided by the National Offensive Cyber Programme. The Chief of Defence Intelligence told the Committee:

> *DI's main budget is not rising in the same way as the Agencies': it will increase from £260.5m in 2010/11 to £307.2m in 2019/20 – the latter figure representing a decrease from 2015/16 spending and approximately flat in real-terms from 2010/11.*[290]

277. We asked DI whether this might reduce its relative ability to support counter-terrorism operations (to which the majority of the Agencies' uplift in funding will be directed), to which it replied:

> *Formal responsibility for CT does not sit with DI. It is the responsibility of MI5 supported by GCHQ and the SIS. The Joint Terrorism Analysis Centre (JTAC) is the focus for analysis of terrorist activity. DI will continue to fund and provide staff to JTAC. DI retains some limited niche capabilities (e.g. imagery support and weapons*

[289] *Not all staff have declared their ethnicity; percentages refer to those who have declared it.*
[290] *Written evidence – DI, 10 July 2016.*

analysis) which provide, and will continue to provide, support to CT elements across government that are involved in operations. We do not judge that the allocation of extra resources to the Agencies will leave DI at a disadvantage.[291]

278. Given that DI does not just support the Ministry of Defence and the Armed Forces in intelligence gathering and analysis, but is also the cross-Government lead on various types of intelligence coverage (such as imagery, geospatial and measurement and signature intelligence), there might be an argument for it becoming the fourth Agency alongside MI5, SIS and GCHQ, with its budget deriving from the SIA. In response to this suggestion, DI said:

*Defence requires its own integral intelligence capabilities, both analysis and collection… Options for closer linkage of DI funding to the [Agencies] were considered during SDSR 2010 and dismissed as being impractical, not least because of DI's core responsibilities to Defence. DI's ability to work with MOD's subordinate headquarters and integrate the requirements ***, will remain vital. The establishment of the Joint Forces Command ensures that DI as a joint enabler is considered coherently alongside other key enablers in Defence.*[292]

Staffing

279. DI's staff numbers are expected to increase from 3,655 at March 2016, to 3,936 at March 2020. We asked DI on what areas these additional staff would be focused:

*Since 2010 DI has acquired new capabilities, some of which came with existing manpower and some which DI is creating from scratch. Between November 2015 (SDSR) and 2020 DI is establishing a number of new capabilities, for example, the Time Dominant Analysis Team, and the Open Source Hub. We will also fully man the new Joint headquarters set up to bring coherence to DI capabilities that work in the electromagnetic environment… Joint Forces Command has given authority for DI to recruit some *** personnel to meet these requirements.*[293]

280. It is notable that March 2016 represents a recent low point in DI's staff numbers. DI explained that it had sought to protect core analytical and operational capability by limiting staff reductions through savings in other areas and, where this was not possible, reducing staff in the corporate services area. In London, the following reductions and savings were made:

- *A reduction in the *** [research and development] programme of about 7.5%;*
- *A reduction in the cost of publishing intelligence and other support;*
- *A package of manpower savings in the [Chief of Defence Intelligence] business support and secretariat functions; and*
- *A small reduction in analytical capability [of] under 10%… some of which anticipated the reduction in requirements on Afghanistan after drawdown.*[294]

[291] *Written evidence – DI, 19 September 2016.*
[292] *Oral evidence – DI, 7 July 2016.*
[293] *Written evidence – DI, 19 September 2016.*
[294] *Written evidence – DI, 19 September 2016.*

Outside London, DI explained staff reductions and savings were made by:

- *Efficiencies arising from the co-location of JARIC [Joint Air Reconnaissance Intelligence Centre] and the then headquarters Intelligence Collection Group at Wyton under PRIDE 1;*
- *The greater use of digitisation at the Aeronautical Information and Documentation Unit;*
- *Reducing some admin support, task management, research, library and geographic collection functions at the Defence Geographic Centre; and*
- *A phased reduction in Meteorological Office and Hydrographic Office programme funding of 10% by 14/15.*[295]

281. DI has informed us that there are gaps in its workforce, but it is relatively sanguine about these:

> *Our man strength today is at around 3,500 military and civilian personnel, split approximately 65 per cent military and 35 per cent civilian. We are currently experiencing about 15 per cent gaps in our civilian positions and about 10 to 15 per cent gaps in our military. The former, civilian gaps, represents the normal churn that one would expect for an organisation of our size. The latter, military gaps, is slightly higher than previously but in line with the [overall] Defence position. We therefore see this as more of a defence issue, broadly, than ours specifically. There are obviously peaks and troughs within each of these.*[296]

Major projects

282. PRIDE 2 will integrate certain capabilities of the Defence Geographic Centre and No 1 Aeronautical Information and Documentation Unit into RAF Wyton, and the Royal School of Military Survey. It is intended to rationalise the estate by removing DI personnel from Feltham, Northolt and Hermitage. At July 2016, likely costs were estimated to be around £65m. This project is at an early stage, with a 'main gate' business case submission likely to take place in late 2018.

283. PRIDE 'One DI' aimed to enhance capabilities at RAF Wyton, by co-locating capability from other DI units, some single Service intelligence units, and representatives from allies and other parts of Government. The project is largely complete and cost £12.5m.

Allocation of effort

284. DI has declared only a minority of its staff as being specifically allocated to individual regions and themes, with the majority described as focusing on specific types of intelligence work such as geospatial and other intelligence collection and analysis, as well as cyber. Many of these are, however, working on particular regions and themes. DI explained:

> *At the moment if we look at resource commitments to *** and then to ***, which includes not just all source analysis but all of our intelligence resources, so*

[295] *Written evidence – DI, 19 September 2016.*
[296] *Oral evidence – DI, 7 July 2016.*

*geospatial [and other collection], *** is around *** [staff] and *** is around ***. As a comparison, *** is around ***.*[297]

285. DI also informed us that it had *** staff working on Syria, Iraq and Islamic State, but explained that its staff are likely to become less and less focused on specific regions as reforms continued and staff worked ever-more flexibly on different areas:

[The fact that those staff are working on Syria, Iraq and Islamic State] doesn't mean everybody else in DI is not doing Daesh at one time or another. As part of our transformation activity, and realigning into more discrete mission teams, around 30 mission teams [have been created]. One of the advantages of that is making specific individuals clearly responsible both for geographic analysis [and] also for thematic analysis.

So in the future we will have a Daesh mission team leader who will be able to pull on different resources as required from other teams… to fulfil a Daesh analysis project problem. In that case we will be able to give [you] a clear idea of what proportion of effort, rather than people, is being put on specific solution sets.[298]

286. DI provides support to a significant number of military operations. When asked how the number had changed since July 2015 – when it was supporting 26 military operations – DI stated that, as at 7 July 2016, this had increased to 89 (27 of which fell under the Commander of Joint Operations and a further 62 managed by other arrangements including NATO and EU operations).[299]

287. DI continues to maintain HUMINT capabilities in support of military operations. These capabilities, which are focused mostly on operational and tactical requirements, ***. DI previously told the Committee that HUMINT staff would increase (to ***) in 2013, but by March 2016 this target was reduced (to ***), at which time the unit was almost one-third below full strength. We questioned the reason behind these fluctuating targets in the space of just a few years and were told:

We have not modified [targets] around anything other than what do we think the requirement is. Now, part of what we have had to do since November last year is look again at the SDSR, look again at a completely different way of measuring outputs and we will review [the latest target] again, as to whether that is the right establishment against a range of tasks…[300]

[297] *Oral evidence – DI, 7 July 2016.*
[298] *Oral evidence – DI, 7 July 2016.*
[299] ****. Oral evidence – DI, 7 July 2016.*
[300] *Oral evidence – DI, 7 July 2016.*

National Security Secretariat (NSS)

Expenditure in 2015/16[301]

Total budget and outturn

£m	Resource spending	Capital spending	TOTAL
2014/15	19.3	n/a	19.3
2015/16	[Not provided]	n/a	[Not provided]

Expenditure by category

- Staff costs: £15.9m
- High-classification IT system: £1.3m

Administration

Staff numbers[302]

	Total staff	SCS	Non-SCS
31 March 2016	151	19	133
31 March 2015	153	21	132

Recruitment in 2015/16

- NSS explained that it does not have a formal recruitment target, and that its recruitment figures cannot be disaggregated from wider Cabinet Office figures.

Staff diversity

At 31 March 2016	SCS	Non-SCS
Female staff	27%	41%
BAME staff[303]	n/a	n/a

Major projects in 2015/16

- Foxhound, a cross-Government project to provide SECRET-level computer systems, for which NSS holds ultimate responsibility

[301] *As reported to the Committee in NSS's end-year report for the 2015/16 financial year. Includes Annually Managed Expenditure (AME).*
[302] *These figures refer to NSS's 'full-time equivalent' headcount.*
[303] *NSS's disclosure rates are too low to produce reliable figures here.*

Policy	
Allocation of effort at 31 March 2016 [304]	• Directorate of Security and Intelligence Policy: 47 staff • Office of Cyber Security and Information Assurance: 29 • Computer Emergency Response Team (CERT-UK): 66

Budget

288. NSS's budget is anticipated to increase substantially from 2015/16, reaching £25.1m in 2016/17 and £27.8m in 2017/18. NSS has explained that this is due to *"a budget transfer from the MoD to the Cabinet Office in support of its broader security and crisis management including the National Security Secretariat (NSS), Joint Intelligence Organisation (JIO) and Cabinet Office Briefing Rooms (COBR)"*.[305] With regard to the mechanics of this transfer, NSS has informed us that *"it will be an annual budget transfer to the Cabinet Office but, for Accounting Officer purposes, we are subject to the Cabinet Office systems, not the MoD systems"*.[306] NSS has informed us that the budget will be spent on:

> *Additional staff [to] respond to crises response, we are revamping the COBR and crisis centres… they are pretty archaic, and we need to upgrade the [video teleconferencing facilities] and things like that. So there is some expansion and investment. We are bringing together, or at least we are enabling, more open source information to be available into the COBR space, which at the moment is purely a highly classified space, and we find that the crises that we are dealing with, actually it is quite useful to have Sky TV on in the background, because, you know, a lot more information comes from them than, say, perhaps from the intelligence agencies in a very fast moving hostage situation, or something, so that is why we are putting some money investing in that.*
>
> *We are setting up a sort of watch keeper 24-hour [Situation Centre] operation, so that we have the capability of responding overnight to crises, which at the moment we don't have at the centre, perhaps surprisingly, the Foreign Office, Defence Intelligence and various others do, but at the Cabinet Office there is not this capability, and we have found that sort of standing up COBRs at 8.00 in the morning, where we could actually have the Prime Minister properly briefed, was quite challenging if there was some crisis overnight.*[307]

---

[304] *The Civil Contingencies Secretariat, Foreign and Defence Policy Directorate, and the Strategic Defence and Spending Review Directorate are omitted from the numbers above as they are not overseen by this Committee. In addition, in October 2016, CERT-UK became part of the new National Cyber Security Centre.*
[305] *Written evidence – NSS, 18 July 2016.*
[306] *Oral evidence – NSS, 13 October 2016.*
[307] *Oral evidence – NSS, 13 October 2016.*

Staffing

289. The two Directorates overseen by this Committee both increased in size during 2016/17:[308]

- The Directorate of Security and Intelligence gained one new post in Counter-Terrorism, three in Strategy and Capabilities, one in Hostile State Threats, and one in Intelligence Policy.
- The Cyber and Government Security Directorate gained five new posts in Hostile State Threats, one related to the National Cyber Security Centre, one on the Agencies' Cyber Activity, three on Cyber and Operations and seven on Government Security.

When asked about these increases in size, the then National Security Adviser (NSA) replied:

> *I don't see it myself as an inexorable trend upwards at the centre… I think it is true that, under the previous Prime Minister, there was a certain accretion of responsibilities at the centre and we obviously responded to that request. The new Prime Minister may approach it slightly differently and, if there are certain tasks that were done by the National Security Secretariat years ago that are no longer needed to be done at the centre, then we will obviously adapt our staffing accordingly.*[309]

290. The vast majority of NSS's staff are there on short-term (two-year) secondments, and this leads to *"a 40 per cent churn in any one year"*.[310] This would appear to lead to a loss of corporate knowledge and lack of sufficient expertise. NSS replied:

> *That is a good question, and it is something that we are looking at, not least in terms of the lessons learned after the Chilcot Inquiry, because they were very critical, the Chilcot Inquiry, of… knowledge management, where records are kept and how we do that… We don't see the Cabinet Office as a… separate department, if you like, like the Foreign Office or the Home Office, it is at the centre of a national security space, and it is a great advantage to the centre to have people that are on secondment from the line departments and it improves the credibility of the centre. It gives us, I think, greater authority and it is of benefit to this wider national security organisation that individuals can have an opportunity to serve at the centre for a limited amount of time. So most of the secondments in are for two, maybe three, years and they gain valuable, you know, experience from working at the centre, but then maybe go back to their own department or go back to another department in the national security space. So as long as that expertise is there within those departments that are members of the National Security Council, I don't think it necessarily matters that they are moving between the Cabinet Office, the MoD, the intelligence Agencies and the Home Office.*[311]

291. We are reassured that secondments and loan can be three years and consider that this should be the norm: two years is too short and such a high level of churn is detrimental to any organisation seeking excellence.

---

[308] *These net increases discount the move of the Government Security Secretariat from the Directorate of Security and Intelligence to the Cyber and Government Security Directorate.*
[309] *Oral evidence – NSS, 13 October 2016.*
[310] *Oral evidence – NSS, 13 October 2016.*
[311] *Oral evidence – NSS, 13 October 2016.*

Major projects

292. NSS is primarily a coordinating not a delivery organisation, and as such we would not expect to see the delivery of major projects within its portfolio. In addition, as a small organisation within the Cabinet Office, we would expect corporate major projects to be run at a departmental level. When asked about its major projects, NSS stated:

> *There are no major projects within the NSS delivery portfolio, however the Director of Security and Intelligence is the Senior Responsible Owner (SRO) for the FOXHOUND Programme… FOXHOUND is a Cabinet Office programme.*[312]

293. The Foxhound programme aims to introduce a new cross-departmental computer system accredited to hold material up to SECRET (but not TOP SECRET) level. It is part of the Government Major Projects Portfolio, which means that it is subject to oversight from the MPA. Given NSS's role as a secretariat, it is odd for it to be running a major IT project. The Committee asked the Director of Security and Intelligence how FOXHOUND fits into NSS's portfolio. In response, he explained that as the Senior Responsible Owner for the project he reports up to the Cabinet Office Permanent Secretary, and that part of the reason it sits in NSS is because it is *"essentially building a capability to protect us from our adversaries"*. He mentioned that such adversaries have the intent and capabilities to compromise less secure Government systems.[313]

294. On the question of whether the technical expertise was available within NSS for such a project, we were told:

> *Yes. So I have a programme director and then I have a team of both contractors, external, lots of IT contractors, I have GCHQ seconded into that team and I also have programme delivery people within that running it as a programme from the Cabinet Office… It is currently for 11 Government Departments but it is [run from NSS] on behalf of the Government.*[314]

Joint working with the Joint Intelligence Organisation

295. A major conclusion of the *Review of Intelligence on Weapons of Mass Destruction*, published in 2004, was that there should be a clear separation between policy creation based on intelligence (which NSS coordinates across Government, supporting the National Security Council) and intelligence analysis (which is led by the JIO). The *Report of the Iraq Inquiry*, published in July 2016, echoed these conclusions.

296. NSS has informed us that in April 2016, it set up a combined support unit with JIO, which will manage finance, staffing and IT matters. NSS suggests, however, that the combination of functions could go further than that, with a joint NSS/JIO Senior Management Board. On this, the then NSA has said:

> *I will make it very clear that, as a result of the Butler Report, there is a very, very clear distinction between the JIO and the NSS and we are very careful to maintain that clear wall between the two functions – the one is assessment and the other is policy formulation. Of course we work very closely together and the NSS sits on the JIC – when the JIC meets, there is an NSS presence and we are often the customer, the intelligent customer for their products. We ask them to do assessments in*

[312] *Written evidence – NSS, 18 July 2016.*
[313] *Oral evidence – NSS, 13 October 2016.*
[314] *Oral evidence – NSS, 13 October 2016.*

particular areas of importance for the [National Security Council], et cetera, but that dividing line is very clear cut.

But what we have found is, as two bodies within the Cabinet Office that actually have quite similar needs in terms of staffing and budgeting, it made sense in terms of efficiency savings to bring together those corporate functions. Now, this is a relatively small number of people. So we have set up a joint sort of management board where we don't discuss any operational issues but we discuss the management aspects of it.[315]

297. Whilst making efficiency savings by amalgamating purely back office functions is commendable, it is important that the sharing of personnel does not creep into policy and analysis staff. We intend to continue to keep this under review.

Allocation of effort

298. NSS had 47 staff in the Directorate of Security and Intelligence Policy at March 2016. Their primary role is to coordinate intelligence and security work. The Director of Security and Intelligence Policy said: *"It is about galvanising a huge volume of work, not duplicating it, but bringing it together into a coherent, coordinated way, to then make sure that the Government goes forward with a clear strategy."* [316]

299. When asked how many NSS staff work directly to support National Security Council meetings, the then National Security Adviser replied:

Well, in one sense all my staff are working to the National Security Council in some way or other… but the sort of administrative stuff is just three people in the National Security Secretariat. But, depending on the subject matter, it may be deploying three or four people from [one of the policy] team[s] to do a lot of the work… depending on the subject matter, because we have a meeting, as you know, of the National Security Council, when there isn't a recess, every week and we are covering basically two subjects every week, very different subjects. So there will be whole processes that are put in place in order to administer that.[317]

National Security Adviser's Principal Accounting Officer role

300. The Principal Accounting Officer (PAO) is the senior official of a public sector organisation whom Parliament can call to account for the stewardship of its resources, as well as having ultimate responsibility for ensuring that sound decision-making and governance processes are in place; in a Government Department, it is usually held by the Permanent Secretary. The NSA is the PAO for the Single Intelligence Account, which is the voted expenditure forming the substantial majority of the Agencies' budgets.[318] It is an odd arrangement given that each Agency is itself headed by a Permanent Secretary-level official, and they are accountable to the Foreign and Home Secretaries, unlike the NSA.

---

[315] *Oral evidence – NSS, 13 October 2016.*
[316] *Oral evidence – NSS, 13 October 2016.*
[317] *Oral evidence – NSS, 13 October 2016.*
[318] *As referred to previously, additional funding may derive from budgets ring fenced for specific projects (such as National Cyber Security Programme funds), overseas partners, from other Government Departments in return for specific services provided (such as secure IT provision), or from the sale of services or intellectual property to the private sector.*

301. The Financial Statement for the Single Intelligence Account 2015/16 explains:

> *Each of the Agencies produces their own Annual Report and Accounts and these are independently audited, in full, by the National Audit Office. The Agencies also produce their own Governance Statements… each Agency operates independently under the direction of its Accounting Officer… The structures in place outlined below… are not formal governance arrangements but complement those of the Agencies.*

It is not altogether clear what the benefits are of the NSA holding this overarching role – particularly given that there appears to be a high level of delegation to Agency Heads anyway. In practical terms, the main mechanism by which it appears that the NSA fulfils his duties is via the 'Financial Steering Group' (which includes the NSA, Agency Heads and Agency finance directors), which the Financial Statement states *"now meets a minimum of three times a year and provides the opportunity for the PAO to meet with his [accounting officers in each Agency] and discuss key financial issues"*. When asked, the then NSA explained that his role was one of high-level oversight:

> *I have sort of formal oversight responsibilities, responsibilities to report to Parliament on how, effectively, whether it is properly and appropriately spent, that money. Now the day-to-day authority for spending the money I delegate to the Heads of the Agencies, as you say, and they have the accounting officer role for that money that is allocated to them. So my role is more one of overall oversight and accountability to Parliament.*[319]

302. Clearly there is a risk that the NSA's role could undermine the authority of the Agency Heads in taking decisions. When questioned on how this works, the then NSA replied:

> *I think it works reasonably well… I see my role more as… challenge and scrutiny, rather than delving into the day-to-day allocation. I am involved in the… upstream allocation of resources between the different Agencies. I do look at the… Single Intelligence Plan that they have drawn up… to ensure… that that fits in with the priorities set by the National Security Council and that the money is allocated against the requirements and priorities set by the National Security Council, but I think it is fair to say that I don't delve into the day-to-day administration of the money. As I say, that is delegated to them as… they are the account holders and they are the… accounting officers for the individual amounts of money.*
>
> *I have not myself found that this has been a difficult process. In the past, there probably would have been some tensions between the three Agencies themselves, to be honest, about the allocation of money, but what has been very noticeable in this Spending Round, and certainly since I have been National Security Adviser, is the amount of joint working that is going on and the fact that they put in a joint bid to the Treasury for resources in the Spending Round, that bid was examined on a number of occasions by the Financial Steering Group, so we reached a situation where I was happy that they were making a reasonable bid to the Treasury, bearing in mind other affordability questions and uplifts of other parts of the national security space we are looking for, and it was extremely impressive how they didn't sort of fall out, arguing about who should get what parts of the cake, but it was a joint bid that went right from the start right up to the final delivery of the amount.*

[319] *Oral evidence – NSS, 13 October 2016.*

So I have not found it a difficult process. I think it gives me enough ability to scrutinise and challenge without actually taking away their own authority as being responsible for their money.[320]

[320] *Oral evidence – NSS, 13 October 2016.*

Joint Intelligence Organisation (JIO)

Expenditure in 2015/16[321]

Total budget and outturn

£m	Resource spending	Capital spending	TOTAL
2014/15	3,515	–	3,515
2015/16	3,456	–	3,456

Expenditure by category

- Operational costs, of which: £3,456,867
- Operational staff costs: £3,276,867
- Other operational costs: £180,000 (exact figure not available)

Administration

Staff numbers[322]

	Total staff	SCS	Non-SCS
31 March 2016	58	6	52
31 March 2015	59	6	53

Recruitment in 2015/16

- JIO explained that it does not have a formal recruitment target, and that its recruitment figures cannot be disaggregated from wider Cabinet Office figures.

Staff diversity

At 31 March 2016	SCS	Non-SCS
Female staff	17%	32%
BAME[323] staff	0%	13%

Major projects

- None.

[321] *As reported to the Committee in JIO's end-year report for the 2015/16 financial year. Includes Annually Managed Expenditure (AME).*
[322] *These figures refer to JIO's 'full-time equivalent' headcount.*
[323] *Not all staff have declared their ethnicity; percentages refer to those who have declared it.*

Policy	
Allocation of effort at 31 March 2016	• Operational: 80%, with precise breakdown of staff number as follows: o Russia and Far East: 7 o Middle East and North Africa: 7 o Africa, Economy and Oil: 7 o Counter-Terrorism, serious and organised crime, and weapons of mass destruction: 10 • Operational support: 20%

Budget

303. Between 2010 and 2016, JIO's budget held steady at around £3.5m, but in 2016/17 it increased to £4.9m and it will rise to £5.2m by 2020/21. In October, JIO informed us:

> *In May [2016], the Chair and the National Security Advisor wrote jointly to the then Prime Minister to request additional funding for investment in HMG crisis response, NSS, and JIO. The Prime Minister was supportive of the investment in JIO; the subsequent uplift process is ongoing and includes the upgrading of IT, new open source capabilities, increased engagement with foreign liaison partners and the establishment of new analytical posts.*[324]

This uplift appears – at least in part – to resource the 'JIO transformation programme', which JIO informed us in July 2016 was:

> *... designed to increase the JIO's ability to meet the all-source analysis requirements of the Prime Minister and the NSC, in line with the recommendations made by [Lord] Butler. It will bring the JIO into line with similar Five Eyes [countries] giving JIO capacity to deliver assessments on the spread of national security issues, including domestic issues, considered at the NSC, to test intelligence against open source data sets and to work more closely with international partners. The transformation programme involves investment in specialist staff and IT...*[325]

304. We asked the Acting Chair of the Joint Intelligence Committee (JIC) for further details and he explained:

> *I think if you look at the size of the JIO, there was an increase in the wake of Lord Butler's inquiry, but actually the numbers then fell back a bit. In the meantime, I think the workload put on the JIO has increased, partly because of the arrival of the National Security Council; partly because, I think, the world has just become a more complicated place. And so that is one part of it.*
>
> *I think the other part of it is very clear recognition that we were no longer at the cutting edge of where we should be. So we looked at some of our international comparators on things, our ability to access open data and that sort of thing; our ability to lead in terms of making sure we are not duplicating strategic assessment*

[324] *Written evidence – JIO, 31 October 2016.*
[325] *Oral evidence – JIO, 2 February 2017.*

across the community; we just were not resourced sufficiently to do that effectively.[326]

These budget increases went against generally constrained public spending, but the Acting Chair defended them as follows:

I mean, you are right: it is in contrast to most of Whitehall, although it is also true that those who supply us with intelligence have that and are going to continue having rising budgets in the same period. So I do not think it is out of kilter with the sort of increases we are seeing in, for example, SIS and MI5.[327]

Staffing

305. JIO has informed us that *"we will have moved from 57 at March 2016 to a target of 80 by March 2017"* – a vast increase of 40% in just one year. These additional staff are intended to produce the increased outputs required as part of the JIO transformation programme. We were given an example of how additional staff will be used on open source work:

there is a lot more open material than there was, say, 10 or 20 years ago. There was an explosion of material, as it were, and there are a lot of quite sophisticated ways in which you can exploit that for analytical purposes… we will have a small team, I think it is four people. They will provide us with a resource, both to do some of the analytics; some of it will be around… mapping and graphics. They will both do some analytics themselves, but they will also be able to provide advice to individual analysts working on a specific area of how they can support their assessment with analytics. So… within JIO there will be a central resource to improve our ability to make sure that all our JIC papers are what they are supposed to do, which is all source and not just classified information.[328]

306. We note that only 32% of JIO's non-SCS staff are female, and just 17% at SCS. Given that JIO's staff are mainly on short-term secondments, it should be possible for its make-up to change relatively quickly with the significant staffing increase. On this, the Acting Chair of the JIC admitted that they needed to do better:

I think one of the issues is that the diversity of some of our feeder organisations is also not high. But I would not want to overegg that, to be quite honest, because as you rightly point out, it… should be easier for us to make a difference in this area. So I think it is something where we will need to make sure, over the recruitment that is going ahead, that we are doing a better job at getting a diverse set of people into the organisation.[329]

Allocation of effort

307. In relation to its allocation of effort, and in particular the question of specialist staff, the Acting Chair informed us:

They are [specialised], but with a degree of flexibility which allows us to balance workloads. So within the Middle East team, there is somebody who leads on Iran, somebody else who leads on Syria, somebody who leads on Iraq. But they box and

[326] *Oral evidence – JIO, 2 February 2017.*
[327] *Oral evidence – JIO, 2 February 2017.*
[328] *Oral evidence – JIO, 2 February 2017.*
[329] *Oral evidence – JIO, 2 February 2017.*

cox, depending on the pressures on the team and the requirements for work to be done.

So – but yes, we try, within reason, to have particular divisions of labour within the teams, which allows them to build up the networks internally and externally of other people in Government and outside, looking at their area and build up a certain expertise without becoming the absolute expert.[330]

Lessons learned from the run-up to the Iraq War

308. The shadow of the run-up to the Iraq War has hung heavily over the JIC: the claim (based on SIS reporting) that Saddam Hussein could launch weapons of mass destruction within 45 minutes was first widely circulated within Government in a JIC Assessment, and it came to public prominence shortly afterwards when it was repeated in a JIC-endorsed Government dossier of September 2002.

309. The *Butler Review on Intelligence on Weapons of Mass Destruction* – published in 2004 – contained numerous recommendations relevant to the JIC. These included recommendations of more caveated language and a better-resourced JIO staff, with an overriding recommendation that the JIC must remain independent from policy-making. On this, the Acting Chair explained that he remained separate from, but liaised closely with, the policy-makers in the NSS:

We are… in adjoining parts of 70 Whitehall, but we are… separate, both in terms of the way in which we do our work, but also the way in which we are addressing issues. We are doing assessment… and they are doing policy… The one thing that… I would just highlight to you… one thing that we have got better at, and I do not think it crosses either Lord Butler or Chilcot… is making sure we are answering the questions policy-makers want. So we have now on the front of a JIC paper what the exam questions were, and we then make sure through our process that the paper underneath that actually answers the questions that policy-makers would like answered, to enable them to look at policy, policy decisions.[331]

JIC Assessments and JIO Intelligence Briefs

310. The JIO's main outputs are JIC Assessments (formal papers which have been cleared by the JIC) and JIO Intelligence Briefs (which are not agreed by the full JIC but are instead approved by either the Chair of the JIC or the Chief of the Assessments Staff). Both types of paper are widely circulated to Ministers, Departments and Agencies – as well as other relevant recipients (including Five Eyes partners) on a case-by-case basis. The vast majority of JIC Assessments and JIO Intelligence Briefs are highly classified.

311. The Committee has, in previous years, been routinely provided with example JIC Assessments and JIO Intelligence Briefs in order to enable its oversight of the JIO's work. This year, however, these were initially withheld (with no reason being formally provided, in contravention of the Justice and Security Act 2013). It was only after three weeks, and the day before the evidence session itself, that it was agreed that the papers would be provided. The papers were finally provided more than seven weeks later. We were subsequently informed that the problem had arisen due to inefficient record keeping by JIO, which led to a delay in establishing that there was a precedent for sharing papers. JIO

[330] *Oral evidence – JIO, 2 February 2017.*
[331] *Oral evidence – JIO, 2 February 2017.*

recognised that there was a delay in doing so and has committed to more timely responses in future. The Committee now has formal oversight of the JIC and JIO and we hope that they will be more forthcoming – in recognition of their responsibilities under the Act – in the future.

Office for Security and Counter-Terrorism (OSCT)

Expenditure in 2015/16[332]

Total budget and outturn

£m	Resource	Capital	TOTAL
2014/15	701.3	78.4	779.7
2015/16	711.7	60.4	772.1

Expenditure by category

- Programme spending: £667.7m
- Administration spending: £44m
- Capital spending: £60.4m

Administration

Staff numbers[333]

	Total staff	SCS	Non-SCS
31 March 2016	551	21	531
31 March 2015	597	26	571

Recruitment in 2015/16

- OSCT recruited 60 staff, against a target of 123.
- This compares with 96 staff recruited in the 2014/15 financial year.

Staff diversity

At 31 March 2016	SCS	Non-SCS
Female staff	17.4%	49.4%
BAME[334] staff	[Not provided]	20.5%

Major projects in 2015/16

- Communications Capabilities Development Programme (CCDP), maintaining communications data and lawful intercept facilities

[332] *As reported to the Committee in OSCT's end-year report for the 2015/16 financial year.*
[333] *These figures refer to OSCT's 'full-time equivalent' headcount.*
[334] *Not all staff have declared their ethnicity; percentages refer to those who have declared it.*

Policy	
Allocation of effort at 31 March 2016	• National Security Directorate: 30% • Communications Capabilities Development: 15% • Counter-Terrorism Protect, Prepare, CBRNE[335] and science and technology: 14% • Strategic Centre for Organised Crime: 11% • Prevent and Research, Information and Communications Unit: 13% • Strategy, Planning and International: 14% • Security industry engagement: 2% • Director-General's office: 1%

Budget

312. OSCT's annual budget has increased by 7% over the past three years, rising from £760m in 2013/14 to £813m in 2015/16. This is expected to increase still further over the next two years, rising to £945m in 2017/18.

313. Given that this has been, and remains, a period of constrained public spending, we questioned OSCT as to the rationale for these budget increases; and what they would be delivering with the additional funding. OSCT told us that the increase in funding was directly driven by the increase in threat and stated:

> *Predominantly [this] is going into the CT police grant… and that includes 34 million this year to build up… our… armed uplift, our ability to counter sort of an attack as we witnessed in Paris.*
>
> *There have also been increases in Prevent and counter extremism which amount to *** million over the SR, sort of allocated over the five years. Aviation security also got an increased investment of *** million and, again, that is responding to the increased threat to aviation security sort of worldwide.*[336]

Staffing

314. OSCT had 551 staff on 31 March 2016, a decrease of 8% from the previous year. This appears to be the result of OSCT missing its recruitment target by over 50%,[337] and a rise in the number of staff departures from 47 (2014/15) to 82 (2015/16). OSCT told us:

> *We have set up a central recruitment hub… because we do need to fill those vacancies… [The] main impediments there are that there is… increased demand across Government… The Brexit departments are vigorously recruiting and they may be the new shiny thing, and therefore are attracting [people], and the second is*

[335] *Chemical, biological, radiological, nuclear and explosives.*
[336] *Oral evidence – OSCT, 3 November 2016.*
[337] *In 2015/16, OSCT was seeking to recruit 123 people, yet only managed to achieve less than half of this number.*

actually [that] our processes are pretty… lumpy in terms of the whole recruitment process. So we have centralised them to try and streamline it.[338]

Major projects

315. OSCT reported that it is running one major project, the Communications Capabilities Development Programme (CCDP). The CCDP aims to maintain and develop the Government's ability to access and utilise communications data (CD)[339] and lawful intercept (LI).[340] OSCT said that the CCDP will *"ensure*[s] *that the police, wider law enforcement agencies and security and intelligence agencies can lawfully obtain, manage and use communications data and intercepted content to: detect prevent and disrupt crime; protect the public and save lives".*[341] The CCDP budget for 2015/16 was £***m, which includes reimbursing CSPs for data retention, paying for specialist staff and developing IT systems.

316. We asked OSCT why the responsibility for running such a programme did not sit within one of the intelligence Agencies. OSCT told us:

The CD services provide evidential quality data. So everything we provide through CD is/can be used as evidence in court. People often say, why isn't the CCD programme delivered by [the Agencies]? Well, we provide evidential quality data and it is fundamentally different. But we do obviously provide service into the [the Agencies] as well.[342]

317. Given that the requirement to sustain these capabilities, and maintain their ongoing development, will continue beyond the end of the current programme, we questioned whether the future element of the CCDP should be delivered by an operational body, rather than a central policy department. OSCT told us that it was considering a number of options, but that some element of the CCDP would remain 'in house':

What we are looking to do as part of the sustainment organisation is to set up a number of groups, one that will look at… change in telecommunications market and the value of different investigative capabilities over time… we are currently working with the operational community, who I think it is fair to say are quite keen to take on that role. We will still maintain policy responsibility within OSCT and strategy to consider the overarching strategy.[343]

---

[338] *Oral evidence – OSCT, 3 November 2016.*

[339] *Communications data (CD) means the details about a communication (the 'who, when, where and how'), but not the content of what was said or written. It applies to telephones (both landline and mobile) and to Internet-based communications (including email, instant messaging, web browsing and social media). CD is central to most Agency investigations. It is used to develop intelligence leads, to help focus on individuals who may pose a threat to the UK, to ensure that interception is properly targeted, and to illuminate networks and associations relatively quickly. The Agencies usually obtain CD in bulk from the communications service providers (CSPs), and equivalent data as a by-product of GCHQ's bulk interception. Alternatively, just as with the police, the Agencies can make a specific request for CD relating to a particular investigation to the CSPs, approved at senior official level.*

[340] *Lawful intercept (LI) refers to the content of the subject's communications and, as a more intrusive capability, is subject to a warrant from the relevant Secretary of State. ***. On receipt of the appropriate authorisation, the CSP will attempt to obtain the relevant content and then direct it back to the Agencies or the police.*

[341] *Written evidence – OSCT, 1 August 2016.*

[342] *Oral evidence – OSCT, 3 November 2016.*

[343] *Oral evidence – OSCT, 3 November 2016.*

318. In June 2015, the CCDP received an AMBER rating from the MPA (defined as, *"successful delivery appears feasible, but significant issues already exist, require management attention. These appear resolvable at this stage and, if addressed promptly, should not present a cost/schedule overrun"*). In November 2016, OSCT told us that this had been upgraded to AMBER/GREEN because: *"[the MPA] felt that we… had good awareness of the risks and had good mitigation plans in place for the array of different risks that have been identified"*.[344]

Allocation of effort

319. OSCT's allocation of effort in 2015/16 was spread across the following areas:

Policy area	**Allocation of effort**
National Security Directorate – provides support to the Home Secretary in her oversight of MI5, and has policy responsibility for investigatory and disruptive powers.	30%
Communications Capabilities Development – aims to ensure that the police and the intelligence and security Agencies can lawfully obtain, manage and use communications data and intercepted content, as discussed above.	15%
Counter-Terrorism Protect, Prepare and science and technology – has responsibility for overseeing the UK's domestic protective security and response plans, including preparation for chemical, biological, radiological, nuclear and explosive (CBRNE) attacks.	14%
Strategic Centre for Organised Crime – responsible for developing and implementing the Government's strategy for combatting serious and organised crime.	11%
Prevent – delivers many of the programmes run under the Prevent strategy, and hosts the cross-departmental Research, Information and Communications Unit.	13%
Strategy, Planning and International – sets the overall context for the UK's Counter-Terrorism and serious crime activities within the respective strategies, provides corporate and operational support, and offers research and analysis capability to the rest of OSCT.	14%
Security industry engagement – coordinates the Government's engagement with the UK security industry to maximise its contribution to national security objectives and promote UK security exports in support of the 'prosperity agenda'.	2%
Director-General's office.	1%

[344] *Oral evidence – OSCT, 3 November 2016.*

LIST OF WITNESSES

Ministers

The Rt. Hon. Amber Rudd MP – Home Secretary

The Rt. Hon. Boris Johnson MP – Foreign Secretary

Officials

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Robert Hannigan – Director, GCHQ

Other officials

SECRET INTELLIGENCE SERVICE

Alex Younger – Chief, SIS

Other officials

SECURITY SERVICE

Andrew Parker – Director General, Security Service

Other officials

DEFENCE INTELLIGENCE

Air Marshal Philip Osborn – Chief of Defence Intelligence

Other officials

CABINET OFFICE

Sir Mark Lyall Grant – National Security Adviser

Philip Barton – Acting Chair, Joint Intelligence Committee

Other officials

OFFICE FOR SECURITY AND COUNTER-TERRORISM

Tom Hurd – Director General, OSCT

Other officials

(List excludes evidence given to the Detainee Inquiry.)

ANNEX A: CODENAMES

Phonetic alphabet name	Original codename
ALFA	***
BRAVO	***
CHARLIE	***
DELTA	***
ECHO	***
FOXTROT	***
GOLF	***

ANNEX B: FULL LIST OF RECOMMENDATIONS AND CONCLUSIONS

A. Individuals returning to the UK after having been fighting in Syria and Iraq represent a significant threat to UK security. We recognise the efforts being made to identify, assess and respond to the return of these people to the UK, and urge the Government to ensure that every returnee is fully assessed, that resources are made available such that appropriate monitoring continues on an ongoing basis, and every effort is made to reintegrate children.

B. The Committee agrees that more must be done to tackle the inspired threat, and welcomes the renewed focus in the latest CONTEST strategy on countering the extremist narrative and helping individuals, particularly those who are most susceptible, to reject radical Islamist ideologies.

C. The joined-up nature of the Agencies' Counter-Terrorism work is an essential development to ensure that duplication is reduced and to focus the collective effort of the Agencies on the most important issues at a time of increased threat. We are increasingly seeing operational benefits from the approach.

D. We welcome the recognition by the Government of the concerns of this Committee and the Independent Reviewer of Terrorism Legislation around the risks associated with the TPIM regime, and the subsequent reintroduction of the relocation element to provide a more effective mechanism for the security services and the police to manage the threat posed in these areas.

E. We commend the efforts of MI5 and the Police Service of Northern Ireland in limiting the number of Northern Ireland-related terrorism attacks. However, at a time when the threat level has been raised, it is important that they are able to maintain the current pressure on the 'new IRA', in particular.

F. Government must work closely with industry internationally to promote the use of modern and secure operating systems in all smart devices connected to the internet. One option could be an accreditation standard for 'approved' Internet of Things (IoT) devices to help guide consumers.

G. The combination of the high capability of state actors with an increasingly brazen approach places an ever greater importance on ensuring the security of systems in the UK which control the Critical National Infrastructure. Detecting and countering high-end cyber activity must remain a top priority for the Government.

H. We welcome GCHQ's offers of assistance and advice to political parties and parliamentarians to improve the security of their networks and data, and encourage all those concerned to accept.

I. Individuals bear responsibility for their own cyber security. A large number of cyber attacks succeed because of basic user errors – such as the use of very simple passwords – and these could be prevented if individuals took sensible precautions and followed National Cyber Security Centre advice, which is available on its website.

J. We welcome GCHQ's work with private companies to improve infrastructure to prevent low-sophistication cyber attacks reaching end-users in the first place.

K. Recruiting and retaining technical specialists in the face of ever-growing levels of private sector competition remains a significant challenge: we encourage GCHQ to develop further innovative ways to ensure that it is able to attract and retain the technical staff so critical to its work.

L. We recognise the importance of offensive cyber capabilities for the national security of the UK, although it will be important in the future to seek international consensus on the rules of engagement and we would support Government attempts to establish this.

M. We note that day-to-day policy responsibility for Hostile State Activity sits with the National Security Secretariat in the Cabinet Office, even though it primarily holds a coordinating function rather than one of policy and delivery. This is symptomatic of the increasing centralisation of intelligence and security matters, which is an issue that continues to cause us concern. Policy on Hostile State Activity may fit more naturally with the rest of domestic-orientated national security policy in the Office for Security and Counter-Terrorism in the Home Office.

N. The events of the past decade or so show that the threat from Russia remains significant. The Agencies' focus on Russia must be maintained.

O. Whilst collaboration with Russia on matters of mutual intelligence interest would be difficult, we agree with SIS that limited lines of communication should be maintained, although a delicate balance is needed.

P. We understand that China's role in relation to Hinkley Point is primarily one of financing, and that operational control remains in UK hands. Nonetheless, we note that the Agencies were consulted in the making of this decision.

Q. Any significant change in US policies relating to detainee treatment would pose very serious questions for the UK–USA intelligence relationship. The US agencies are well aware of the implications for cooperation with the UK and other allies, and the UK Agencies are monitoring the situation closely. The UK Government must continue to keep a close eye on any changes in US policy and take swift action if there are signs that these might run counter to British laws and values.

R. We are encouraged that the Government has taken forward this Committee's recommendation on data sharing with US communications service providers. We are, however, concerned at the length of time it is taking to make progress. Given the goodwill towards this legislation, which the Committee discerned on its visit to Washington, we urge the Government to renew efforts to pursue this matter with its US partners.

S. European mechanisms play an essential role in the UK's national security, particularly at a time when the Agencies have all emphasised the importance of enhancing their cooperation with European counterparts. We urge the Government to be more forthcoming with its assessment of the associated risks of the UK's impending departure from the European Union, and the mitigations it is putting in place to protect this vital capability.

T. In particular, it is in the overall interests of European security that the UK Agencies retain full access to European data sources and continue cooperation on law enforcement and intelligence. Ensuring that such access and cooperation can continue post-Brexit should be a priority for both the UK and the EU. Once the UK has left the EU, intelligence cooperation is an area where it can continue to be a leader amongst its European allies.

U. The Agencies receive a significant proportion of their funding from sources other than the Single Intelligence Account. Many of those funding streams are for work on areas such as cyber security, offensive cyber programmes, counter-terrorism projects, and capability building with key partners overseas, which could well be considered 'core' business. We recommend that such funding is incorporated into the Single Intelligence Account. This will reduce complexity, provide greater certainty of funding, aid good financial management, and increase transparency for Parliament and the public.

V. In recent Spending Reviews there has been a tendency to claim savings benefits and efficiencies against rather intangible concepts, or by abandoning future projects that may have only been aspirational. This has led us to question the validity of claimed savings. There is no doubt that the savings required within the current Spending Review period are very substantial and without their successful delivery a number of critical investment projects will need to be cancelled. One year into the Spending Review period, some progress is being made, but there is still no plan for the total savings required over the whole period. When we return to this subject next year it is imperative that the Agencies have a full plan for the delivery of the full savings required. We will invite the National Audit Office to work with us next year to analyse the savings programme in greater detail.

W. We are reassured that staff of all three Agencies have a number of routes to discuss moral, ethical, policy, legal or any other concerns, and that these appear to be reasonably well utilised. We were also interested to hear from Agency Heads that staff have been told that the ISC is an approved route for whistleblowing whilst protecting the secrecy of their work. We fully support this, but note that if the Agencies intend it to be used then the current bar on Agency staff being able to communicate with the Committee directly via secure email will need to be removed.

X. Whilst we accept that there will remain a need, on occasion, to buy in specialist skills from outside, we nevertheless welcome initiatives to reduce reliance on time-hire contractors in circumstances where permanent staff are a more suitable and cost-effective option. Given the considerable growth in the number of time-hire contractors, and the costs involved, we recommend the National Security Adviser, as Principal Accounting Officer for the Single Intelligence Account, reviews use of permanent staff versus time-hire contractors focusing on the skills required, flexibility needed and costs involved (including the feasibility and value of delivering services in house).

Y. The Agencies' primary business is information: everything they do is underpinned by their ability to record, maintain and use that information properly. The ALFA programme is crucial to MI5's core business of managing information. The programme has faced major problems since its inception and there remain significant risks to its successful delivery, despite some positive efforts from MI5 over the last year. It is essential that this programme, and other information management programmes being put in place across the UK intelligence community, succeed.

Z. The management of GCHQ's accommodation has long been an area of serious concern to this Committee. We note GCHQ's adoption of a new approach, which seeks to address not only its lack of physical space, but also its diversity issues, and will examine whether or not it provides a coherent solution in due course.